Elecciones y ciberseguridad

Félix Arteaga | Investigador principal, Real Instituto Elcano | @rielcano

La protección de las leyes y sistemas electorales de los países democráticos no se habían diseñado para prevenir ciberataques. Hasta hace poco era impensable creer que se pudiera influir en las elecciones, perturbando o impidiendo su realización mediante ciberataques o condicionando el sentido del voto de los electores mediante operaciones de influencia, desinformación y propagación de noticias falsas y de información obtenida de forma fraudulenta. Sin embargo, lo ocurrido en varios procesos electorales como el de la Presidencia de Estados Unidos en 2016 o el de las elecciones generales de Holanda en 2017, donde se registraron operaciones cibernéticas de influencia unido a la proximidad de elecciones legislativas de Estados Unidos en noviembre de 2018, y al Parlamento Europeo en mayo de 2019, han disparado las especulaciones sobre la fragilidad de los sistemas electorales ante las manipulaciones cibernéticas.

Partidos políticos como la Unión Demócrata Cristiana de la canciller Merkel, el movimiento En Marche! del Presidente Macron o el Partido Demócrata de Estados Unidos han tenido amargas experiencias con los ciberataques. No son hechos aislados sino que se corresponden con un patrón de desinformación que se achaca a países como **Rusia**, según un Informe del Comité de Asuntos Exteriores del Senado de enero de 2018, pero que pudieran ser imitados por **otros actores estatales** o no en el futuro. Se aprovechan situaciones de confrontación interna o enfrentamientos electorales para debilitar la credibilidad de los sistemas democráticos o de las personas que los representan. Se toma partido para satisfacer unos intereses geopolíticos, geoeconómicos o ideológicos determinados. De ahí el estado de preocupación que se percibe en los medios políticos y de comunicación y al que los expertos en ciberseguridad tratan de aportar soluciones. El debate sobre la participación o no de los servicios secretos rusos en las elecciones presidenciales de 2016 ha aumentado la expectación en torno a la ciberseguridad, lo que se refleja en la proliferación de noticias en los medios de comunicación y en la multiplicación de las comparecencias de las autoridades responsables. No se puede descartar que se produzcan y se debe demostrar que se han tomado todas las medidas posibles para evitarlo.

“Se aprovechan situaciones de confrontación interna o enfrentamientos electorales para debilitar la credibilidad de los sistemas democráticos o de las personas que los representan”

La dependencia tecnológica de los sistemas electorales facilita su alteración cibernética. A la preocupación de los responsables de esos sistemas por proteger los datos del censo, la organización y recuento de las votaciones, se une ahora la de los candidatos y partidos políticos por evitar que el robo de información sensible sobre ellos, sus donantes o simpatizantes. Se enfrentan a un problema ajeno a la cultura política democrática y pasará mucho tiempo y muchos ataques antes de que se tome conciencia de su necesidad. Si las empresas importantes han tardado años en mentalizarse de los

riesgos de ciberseguridad que afrontan, no se les puede pedir a quienes organizan, se postulan o votan en las elecciones que adopten medidas de protección tan sofisticadas y costosas como ellas. Tampoco se puede pedir a los gobiernos y a las administraciones públicas que eviten las injerencias y ataques porque sus medios son limitados y tienen que dar prioridad a los objetivos de mayor riesgo como las infraestructuras críticas o los servicios públicos esenciales que también pueden ser objeto de ciberataques.

En consecuencia, los responsables de supervisar la ciberseguridad de las elecciones están elaborado recomendaciones básicas que no garantizan la protección total, pero, al menos, contribuyen a mentalizar a los implicados y reducir su vulnerabilidad. En este CIBER Elcano se incluyen dos documentos de reflexión sobre el problema. Uno procede del Grupo de Cooperación NIS de la UE y el otro del Consejo de Seguridad Nacional de los EEUU. En el primero: Compendium on Cyber Security of Elections Technology, publicado en julio de 2018, se resalta la preocupación de que un ataque durante las elecciones al Parlamento Europeo sobre un solo país (el eslabón más débil) podría alterar el reparto de escaños del total de las votaciones. El Informe contiene las mejores prácticas conocidas ante los incidentes electorales pasados, pero la decisión de adoptarlas corresponde a cada uno de los Estados miembros. La Comisión no puede entrar a regular las medidas nacionales y, de hecho, ha descartado regular la desinformación para evitar conflicto con las normas nacionales y con principios tan sensibles como la libertad de información.

“La Comisión Europea ha descartado regular la desinformación para evitar conflicto con las normas nacionales y con principios tan sensibles como la libertad de información”

El segundo: Cybersecurity Campaign Playbook recoge también recomendaciones para los responsables de las campañas electorales en los Estados Unidos, con el fin de que adopten **las medidas de seguridad más elementales**. Los riesgos varían desde los robos de correos con información sensible a la perturbación de las encuestas, los contactos o la captación de fondos para las campañas. Son riesgos acentuados por la progresiva digitalización y automatización de las mismas, lo que aumenta su vulnerabilidad a los ciberataques. La combinación de *trolls*, redes sociales y medios de comunicación sensacionalistas genera desinformación viral que afecta a la intención electoral.

Los grandes proveedores de servicios digitales como Microsoft, Facebook o Google, junto con las empresas de ciberseguridad están participando en la campaña de concienciación y tomando medidas. Sin embargo, esas medidas no pueden prevenir la totalidad de ataques, especialmente los de naturaleza geopolítica, porque las empresas no pueden dejar de prestar servicios esenciales para su modelo de negocio aun a riesgo de facilitar la actuación de los hackers maliciosos o de los servicios de inteligencia. Pueden cerrar, como ha hecho Microsoft, algunos dominios desde los que operaban proxies rusos como Fancy Bear (APT28) o clausurar cuentas falsas como ha hecho Facebook para prevenir interferencias, pero difícilmente pueden evitar que se vuelvan a abrir o que cambien de modo de actuación si hay detrás intereses geopolíticos.

Los medios de comunicación también se han visto implicados en la defensa de la trasparencia electoral y contribuyen a la mentalización de los votantes, pero las

redacciones tienen que elegir entre llevar a cabo todas las comprobaciones necesarias o perder la primicia. La **tensión entre la información veraz y la información rentable** es mayor entre los medios digitales cuya fuente principal de ingresos depende de la cantidad y no de la calidad del flujo informativo que generan. La financiación mediante ingresos de publicidad (online advertising market) ligados al volumen de flujos incentiva la despreocupación por la calidad de la información. Ya que las noticias sorprendentes, morbosas o negativas atraen más lectores, las redacciones estimulan esas noticias al borde o dentro de la posverdad, habitualmente sobre personalidades o asuntos conocidos o controvertidos, pero que también pueden aprovechar esas 'habilidades' en los procesos electorales.

Vivir en democracia no es fácil. Lo ha sido en algunos momentos, pero los enemigos de la democracia (lideres autoritarios, hackers sin ética, politólogos sin escrúpulos o accionistas mediáticos) han encontrado en el ciberespacio un instrumento de acoso a los procesos electorales. En el pasado, han cogido a los procesos electorales por sorpresa y podrán volver a intentarlo. Pero esta vez no será ya una sorpresa ni tendrán tanto éxito si todos los implicados asumen su cuota de responsabilidad.