Desinformación, elecciones y ponencia: la ciberseguridad está de moda

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

En el mes de marzo, la ciberseguridad española ha cobrado actualidad debido a la inminencia de los procesos electorales –el primero, el 28 de abril–, que ha puesto sobre la mesa la necesidad de prevenir los riesgos asociados con la desinformación y la fiabilidad de los sistemas electorales. También porque la Comisión Mixta de Seguridad Nacional acaba de publicar sus conclusiones sobre el estado de la ciberseguridad en España tras las comparecencias en ella de responsables y expertos del sector.

"[la] ciberseguridad española ha cobrado actualidad debido a la inminencia de los procesos electorales, (…) que ha puesto sobre la mesa la necesidad de prevenir los riesgos asociados con la desinformación y la fiabilidad de los sistemas electorales".

Yendo por partes, la preocupación por los riesgos del ciberespacio asociados a los procesos electorales ha cobrado vigencia con la llegada de las elecciones. Hasta entonces, la preocupación gubernamental por la ciberseguridad de los procesos electorales ha sido limitada debido a la fiabilidad de las medidas tecnológicas asociadas al proceso de transmisión y recuento de las papeletas, que se depositan física –y no electrónicamente– en las urnas. La ausencia de incidentes en las convocatorias electorales previas, incluidas las autonómicas catalanas de diciembre de 2018, ha evitado la necesidad de adoptar medidas excepcionales como han hecho otros Gobiernos. La preocupación ha sido mayor en relación con la posibilidad de que se utilice el ciberespacio para influir en el voto de los ciudadanos mediante campañas de desinformación y propaganda (ver el "Informe de Buenas Prácticas sobre desinformación en el ciberespacio", elaborado por el Centro Criptológico Nacional y reseñado por el *CIBER elcano* de marzo de 2019).

En su edición de abril, el *CIBER elcano* recoge una valoración conceptual de la desinformación a cargo de su responsable, Julia Alicia Olmo y Romero, como embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad. Tanto su ARI como el de Carlos Galán Cordero describen las medidas adoptadas por los Gobiernos europeos –incluido el español–, medidas que se amplían con las recogidas en el informe del Parlamento Europeo sobre desinformación y propaganda en la UE y sus Estados miembros, que se adjunta en esta edición.

Los medios de comunicación se han hecho eco de las medidas adoptadas por el Gobierno en marzo para prevenir dichos riesgos, tanto los que afectan a la seguridad de los sistemas informáticos asociados al proceso electoral como los vinculados a las acciones de influencia (*fake news*). Para lo primero se han incrementado las exigencias técnicas de los pliegos de contratación y se han llevado a cabo auditorías previas a las

empresas encargadas del recuento. Para afrontar los intentos de desinformación, se ha creado un grupo de seguimiento dentro de la Secretaría de Estado de Comunicación de Presidencia del Gobierno.

En segundo lugar, la Comisión Mixta de Seguridad Nacional acaba de publicar el "Informe de la ponencia para el estudio de la ciberseguridad en España", que ha elaborado entre septiembre de 2017 y marzo de 2019 y en el que se recogen resúmenes de las comparecencias de responsables y expertos y las conclusiones de la Comisión. Las comparecencias son más interesantes y extensas que las conclusiones, que se limitan a codificar el estado de la ciberseguridad hasta el cierre de la legislatura y a proponer algunas medidas genéricas relacionadas con lugares comunes como la necesidad de mejorar la cultura, la educación, la cooperación público-privada, los presupuestos o la base industrial de la ciberseguridad, recomendaciones que se reenvían a la futura Estrategia de Ciberseguridad Nacional. Precisamente, en la última de las comparecencias, el presidente del Consejo de Ciberseguridad Nacional, Félix Sanz, informó a los miembros de la Comisión que la nueva estrategia ya estaba cerrada.

Continúa abierto el debate sobre la seguridad –y el negocio– de las redes 5G, que ya hemos analizado en el *CIBER elcano* de marzo. España y el resto de los Estados miembros de la UE deberán tener en cuenta la recomendación sobre la ciberseguridad de las redes 5G que acaba de emitir la Comisión para armonizar las decisiones nacionales y asegurar la conectividad de sus infraestructuras digitales a partir de 2020 mediante el Plan de Acción 5G.

Otro debate que se abre, y sobre el que va a trabajar el Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano, tiene que ver con la creciente complejidad operativa, tecnológica y jurídica a la que tienen que hacer frente las Fuerzas y Cuerpos de Seguridad del Estado y la Fiscalía en el curso de las investigaciones policiales y judiciales (interceptación de comunicaciones, captación y grabación de comunicaciones electrónicas, captación, grabación y localización de imágenes, registro *in situ* y en remoto de equipos informáticos, etc.), una dificultad ya adelantada por Javier Alonso Lecuit en *CIBER elcano* y que puede verse acrecentada con nuevas arquitecturas de información y tecnologías, tales como la virtualización de redes, dispositivos o los nuevos paradigmas asociados a las redes 5G. En el mismo sentido, la Comisión recomendó, en febrero de 2019, iniciar negociaciones con Estados Unidos y actualizar el Protocolo de Budapest para la obtención de pruebas electrónicas. Además, acaba de completar las medidas adoptadas en el Reglamento de diciembre de 2018 sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (Reglamento e-Evidence) mediante una directiva para designar a los representantes legales para la obtención de pruebas.