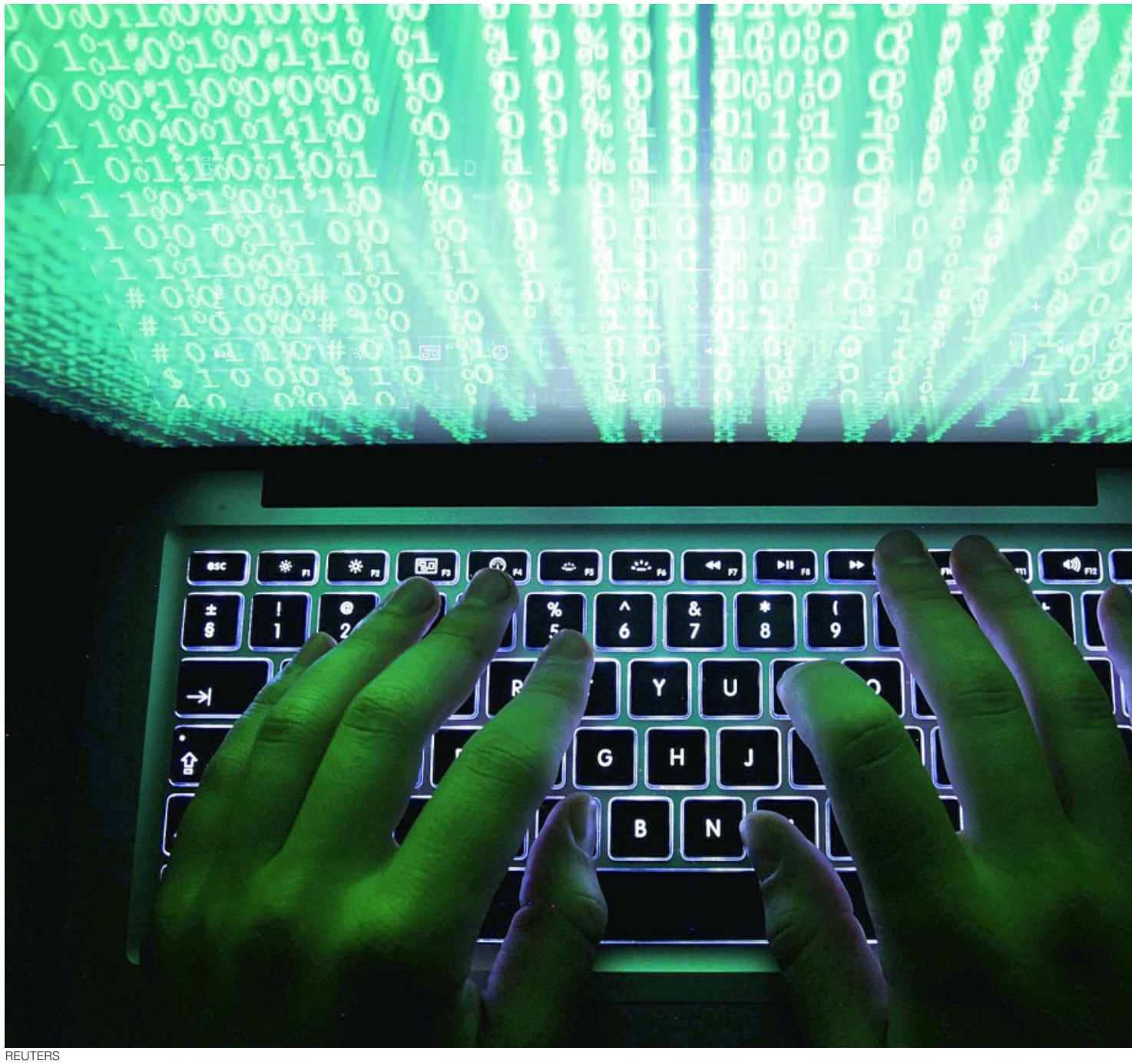

REUTERS

EL NUEVO CAMPO DE BATALLA

Hacke (mate) a las democracias

POR
ÁNGEL VALLEJO
Director de RRII de THIBER, the Cybersecurity think tank

El pasado año ha estado repleto de incidencias relacionadas directa o indirectamente con las tecnologías de la información y la comunicación (TIC). "Wannacry" puede sonar a estas alturas como un ciberataque lejano, si atendemos a "Meltdown", a "Spectre" y al enorme problema que nada más empezar 2018 se ha puesto sobre la mesa. Lo digital, lo cibernético, lo permea todo. Es el vehículo de la mayoría de las actividades que implican relaciones sociales, políticas y económicas. Vivimos en digital y nuestra inmersión es tal que, salvo que se haga un esfuerzo consciente cada cierto tiempo para cuestionar o replantear sus usos, nos resulta casi invisible. Es esa característica vehicular la que hace a las TIC tan indispensables como omnipresentes. Junto a ello, ocurre que su disponibilidad sólo se valora debidamente cuando se está en riesgo de perder-

La ciberseguridad se ha convertido en los últimos tiempos en una preocupación capital para todos los gobiernos

la. En las numerosas ocasiones en que los sistemas, individuales o empresariales, sufren un revés, se pone de manifiesto una doble cuestión: por un lado, la dependencia casi absoluta de las TIC en todos los ámbitos y, por otro, la perenne exigencia de actualizar los sistemas construidos por y sobre esas TIC.

Los ciberataques a las estructuras de algunas compañías que, entre otras cosas, son supuestamente símbolo y garantía de la seguridad de los clientes a los que sirven genera seria preocupación. El "hackeo" de cuentas gubernamentales, militares o no, y el compromiso o exposición de los sistemas de estructuras como el Pentágono, la Comisión Europea o algunos de los más conocidos bancos a nivel mundial, hacen que inevitablemente se plantee si no estaremos, como sociedad, demasiado expuestos a los riesgos TIC. De manera paralela y casi inevitable se suscita el debate sobre una suerte de paso atrás, de apartamiento de la carrera perpetua por la actualización de los sistemas. El tema no es menor. El coste de actualización de los sistemas TIC se ha convertido en una de las mayores (si no la mayor) partida de inversión de capital por parte de las compañías de los estados industrializados, con una recurrencia que obliga a pensar hasta qué punto dicha inversión genera realmente un retorno efectivo, habida cuenta del ritmo de innovación de dichas tecnologías. Es decir, se invierten cantidades cada vez mayores en construir sistemas TIC, que hay que implementar y mantener puntualmente actualizados, presentando esos mismos sistemas un horizonte de obsolescencia preocupantemente corto.

Mientras que en compañías o actividades de ámbito esencialmente digital (empresas de software, de comercio en internet, de seguridad informática, telecos y redes sociales) ese ciclo temporal es consustancial al propio curso de su negocio, para las empresas o profesionales que son solo usuarios de las TIC el escenario actual genera tensiones tanto operativas como de estrategia. El impacto económico y organizacional que genera el actual modelo es relevante, y buena parte de esas tensiones surgen al contraponerse el coste de las inversiones (capital, tiempo y recursos humanos) con la certeza de que no puede garantizarse la seguridad total. Si después de esfuerzos, inversiones y modificaciones operativas y en las relaciones con sus clientes u otros sujetos de interés las organizaciones no están exentas de sufrir ciberataques o bloqueos causados por problemas intrínsecos de la red, ¿tiene sentido someterlas a un proceso continuo de renovación y actualización perpetuo, con las consecuencias que genera la natural resistencia al cambio en las organizaciones? Y, en todo caso, ¿es factible, o simplemente posible, adoptar una posición de paso atrás ante los retos y riesgos asociados a las TIC?

LA INVERSIÓN DIGITAL QUE ASUMEN LAS EMPRESAS Y GOBIERNOS CHOCA CON LA CERTEZA DE QUE NO EXISTE UNA SEGURIDAD TOTAL

No es nuestro objetivo afrontar aquí extensamente las cuestiones planteadas por autores como el apocalíptico Andrew Keen, Jaron Lanier (uno de los padres de la realidad virtual, que incide en el lado menos luminoso de las TIC), o Nicholas G.Carr, que simplemente niega la relevancia estratégica de estas tecnologías, una vez que se han hecho accesibles a la gran mayoría de los ciudadanos y organizaciones. Pero, sin entrar en la bondad o error de dichas hipótesis, sí parece sensato mantener que las posturas directamente neoluditas respecto de las TIC no resultan sostenibles en nuestro entorno. »

LAS HUELLAS DEL WANNACRY

Fuente: AFP

Infografía LA RAZÓN

Por un lado, ciudadanos y empresas consideran muy relevantes tanto los avances tecnológicos como la necesidad de adaptar los sistemas a la cambiante realidad y a los riesgos aparejados. La Encuesta Mundial sobre el Estado de la Seguridad de la Información muestra que, desde 2012, el presupuesto medio que las compañías dedican a ciberseguridad en el mundo casi se ha duplicado, pasando de 2,8 a 5,1 millones de dólares. En España, la inversión de las empresas en seguridad de la información ha evolucionado de manera pareja, pasando de 3,1 a 3,9 millones de dólares de media. Por otro, las administraciones, desde las locales hasta las supranacionales, muestran su preocupación y, más importante, su ocupación en la materia TIC. En Europa, la implementación de la directiva 2016/1148 NIS está generando ya cambios relevantes en las compañías afectadas, y el Reglamento de Protección de Datos (GDPR, en sus siglas en inglés) será aplicable en mayo de 2018. Los estándares de protección del derecho a la intimidad, a la información y a la libre difusión de ideas están cada vez más indisolublemente vinculados al uso de medios técnicos digitales. A la vez, aumentan las obligaciones y garantías que deben asumir los actores del entorno TIC.

EUROPA VA A DESTINAR 6.000 MILLONES EN DIGITALIZACIÓN, ENTRE ELLOS 1.000 EN SEGURIDAD. UN PASO ATRÁS ES INVIABLE

Compañías cuyos servicios son indispensables para una buena operativa TIC están sometidas a la posibilidad de graves sanciones en caso de incumplimiento de las obligaciones de la directiva NIS, cuya trasposición en España se encuentra prácticamente lista para su operatividad el 9 de mayo de 2018 (su anteproyecto se publicó en diciembre de 2017). Se trata bien de empresas proveedoras de servicios digitales, bien de operadoras de sectores críticos (energía, banca, salud…). Todo esto supone, para este tipo de compañías, y derivadamente para sus clientes, corporativos o particulares, la necesidad de estar continuamente actualizando sus sistemas y protegiéndolos frente a amenazas intrínsecas y también externas.

El nivel de identificación de la UE con la global tendencia potenciadora de las TIC y, a la vez, de la protección ante los aspectos generadores de riesgo de las mismas, queda plasmado en las agendas de los grandes eventos europeos. El programa HORIZON 2020 de la Comisión Europea prevé, solo para el periodo 2018-2020, una inversión en investigación e innovación de la digitalización europea de 6.000 millones de euros. Solo para la parte de ciberseguridad (un área que el presidente de la Comisión Europea, Jean-Claude Juncker calificó como prioridad clave) se dedicarán 1.000 millones.

El área conocida como FET (Future and Emerging Technologies) se ve muy potenciada, teniendo como objetivo desarrollar ideas novedosas y su implementación a través de tecnologías radicalmente nuevas, tal y como las define el programa. De otro lado, se mantiene como prioritaria la investigación para posibilitar unas infraestructuras digitales (e-infrastructures) sólidas y resilientes. Hay otros riesgos e inquietudes. La iniciativa de la Comisión respecto de las "fake news", plasmada en su "Consulta pública sobre noticias falsas y desinformación en línea", activa hasta el 23 de febrero de 2018, evidencia que los retos actuales se multiplican.

Es imprescindible, ciertamente, buscar un equilibrio entre la omnidigitalización de las relaciones sociales, económicas y políticas y el rechazo a la necesaria adecuación a la tecnología. Pero los dos elementos antes señalados (la percepción de ciudadanos y empresas junto a los citados avances y proyectos de la UE) hacen inviable asumir la mera posibilidad de un paso atrás a la hora de sumergirse en la tendencia a profundizar en las tecnologías digitales. LR

CERCO A LAS "FAKE NEWS" LA DEMOCRACIA

Las noticias falsas se han convertido *en el máximo exponente de la posverdad en un mundo en el que gran parte de la sociedad, especialmente los jóvenes, se informa a través de Twitter y Facebook principalmente. Ejércitos de cibernautas inventan, difunden e influyen en procesos electorales a través de mensajes y "fake news". Las grandes compañías tecnológicas se han comprometido a combatir este mal del siglo XXI.*