El reto de la India

Enrique Fojón Chamorro

Ingeniero Superior en Informática y miembro del Instituto Español de Ciberseguridad (SCSI) de ISMS Forum

Desde hace años, y por múltiples razones, la India centra la atención de los analistas políticos, de seguridad y defensa, económicos y tecnológicos de la comunidad internacional.

La India, desde el punto de vista geopolítico, soporta un frágil equilibrio que condiciona no solo su seguridad y defensa sino la de gran parte del continente asiático y, por extensión, la del resto del mundo. Los conflictos territoriales y religiosos con sus países vecinos, Pakistán y China, así como la cercanía e influencia de la guerra de Afganistán, unido a la necesidad de las 'potencias occidentales' de disponer de un aliado fiable en Asia, refuerzan su importancia estratégica. En lo referente a su política interior, la India afronta problemas muy heterogéneos que van desde la creciente demanda energética de un país en expansión a los conflictos de carácter religioso entre las comunidades hindú y musulmana del país.

Por otra parte, en 2020, según todas las previsiones, la India será el país más poblado del planeta, así como la segunda economía mundial. Estas previsiones no han pasado desapercibidas para los gobiernos de Estados Unidos, Rusia o Alemania que están trabajando en el fortalecimiento de sus relaciones comerciales, económicas y culturales con la India.

Pero, ¿cuál es el papel del ciberespacio en el complejo presente y futuro de la India? A lo largo del presente artículo se pretende arrojar algo de luz a esta cuestión.

La 'India moderna', con las TIC

Tras la independencia del Imperio Británico, Jawaharal Nehru, primer ministro de la India entre 1947 y 1964, otorgó a las ciencias y la tecnología un papel protagonista en la identidad de la 'India moderna'. La creación de una red de universidades y escuelas destinada a la formación de los futuros talentos científicos y tecnológicos del país fue una de las primeras medidas adoptadas por su gobierno. El máximo exponente de esta red lo constituyen los 16 Institutos Indios de Tecnología (IIT) repartidos a lo largo y ancho del país. La importancia y prestigio de los IIT en la sociedad india se refleja en que solo uno de cada 50 jóvenes que aspiran a formarse en ellos consiguen su objetivo.

> El ciberespecio específico de India está muy lejos de un estado de riesgo conocido y controlado

Del mismo modo, la India fue pionera en la creación de organismos de gestión y control tecnológicos. En 1975, el gobierno indio creó el Centro Nacional en Informática (NIC, por sus siglas en inglés) con el objeto de proporcionarle soluciones TIC. Durante el trienio 1986-1988, el NIC coordinó e impulsó la puesta en marcha de las tres primeras redes de telecomunicaciones de la India: INDONET, que interconectaba los grandes *mainframe* IBM de la Administración; NICNET, cuya función era interconectar todas las delegaciones del NIC repartidas por el país; y ERNET, que interconectaba las instituciones académicas que fomentaban el I+D+i en la India.

En 1998, la India fue igualmente pionera al aprobar la *Internet Act*, a través de la cual se reconocía la importancia estratégica de Internet para el desarrollo global del país.

Durante la primera década del siglo XXI, el gobierno indio creó un conjunto de organismos destinados a la dirección, gestión y seguridad de su ciberespacio. Entre estos organismos destacan el National Information Board (NIB), responsable de la política estatal en materia de ciberseguridad; el National Information Infraestructure Protection Centre (NIIPC), responsable de la seguridad TIC de las infraestructuras criticas del país; y el CERT-In, el centro operativo de respuesta a incidentes cibernéticos.

Situación actual del ciberespacio

A pesar del compromiso histórico con las TIC y los esfuerzos realizados por el gobierno indio, su ciberespacio específico no dispone de una infraestructura TIC madura y su nivel de ciberseguridad se encuentra muy lejos de un estado de riesgo conocido y controlado. Esta realidad es común a la mayoría del ciberespacio del resto de naciones, aunque en el caso de la India es aun más compleja debido a su vasta extensión geográfica, su elevada población y su compleja situación geopolítica.

A pesar de las dificultades, el ciberespacio indio crece a un ritmo lento pero sostenido como demuestran los siguientes datos:

1) El sector de las TIC aportó un 6,4 por ciento al PIB de la India durante 2011, lo que supone un incremento del 33 por ciento respecto a la contribución en 2006.

2) Durante 2011, la inversión en I+D+i fue del 0,7 por ciento del PIB. Casi el 70 por ciento de esta inversión fue realizada por el Estado.

3) 149 operadores de servicios de internet y telecomunicaciones proporcionan acceso a Internet y telefonía móvil a una población potencial de 800 millones de personas, aproximadamente el 75 por ciento de la población india.

4) El diez por ciento de la población tiene acceso estable a la banda ancha. Las previsiones sitúan este porcentaje en el 14 por ciento en 2016.

5) La India ocupa los primeros lugares, por número de usuarios, en servicios tan populares en Internet como Gmail, Yahoo, Facebook o Twitter.

6) Durante 2011 el comercio electrónico ha experimentado un crecimiento medio del 47 por ciento respecto a 2008.

7) Según el *Cisco Visual Networking Index*, se prevé un crecimiento importante en el tráfico de internet en la India pasando de los actuales 1,6 Exabytes a 13,5 Exabytes en 2015.

Desde el punto de vista organizativo, el gobierno indio dispone de un conjunto de órganos y organismos con competencias en la dirección, gestión y seguridad de su ciberespacio. En teoría, estos organismos trabajan de manera integrada y coordinada bajo las directrices del National Information Board (NIB), órgano que aglutina a representantes de los principales ministerios, fuerzas armadas y servicios de inteligencia del país. En la práctica, cada organismo trabaja de manera autónoma, lo que redunda en un desconocimiento del estado de situación del ciberespacio indio, así como del global, una ausencia de procedimientos que posibiliten una compartición efectiva de información entre los diferentes actores involucrados en la ciberseguridad nacional, una ausencia de políticas coordinadas en I+D+i, así como un ineficaz marco de colaboración público-privada.

A nivel legislativo, la *IT Act* de 2008 regula las competencias del gobierno en la dirección, gestión, control y seguridad del ciberespacio indio, la *Copyright Act*, todas las cuestiones relacionadas con la propiedad intelectual y la *Data Protection Act,* todo lo relativo con la protección de datos.

En el ámbito educativo, el gobierno indio ha apostado por la captación y formación de ciber-talentos en los IIT del país. Sin embargo, esta ambiciosa apuesta no ha alcanzado los resultados esperados. Cerca del 70 por ciento de los licenciados en los ITT que posteriormente cursan sus estudios de postgrado o doctorado en los Estado Unidos o Europa no regresan a la India. Esto se debe a la falta de proyectos TIC estables y, sobre todo, a las excepcionales condiciones laborales que les ofrecen las principales compañías y universidades estadounidenses y europeas.

La India ocupa los primeros lugares, por número de usuarios, en servicios tan populares en Internet como Gmail, Yahoo, Facebook o Twitter.

La política de ciberconcienciación tampoco está siendo efectiva. La falta de medios y la cesión de las competencias educativas a cada una de las regiones del país impiden la implantación de esta política.

En el ámbito de las Fuerzas Armadas y los servicios de inteligencia existen iniciativas en materia de ciberseguridad destinadas a la creación de un conjunto de CERT dotados de capacidades defensivas y ofensivas. Los ejércitos indios disponen de unidades cibernéticas pero sus capacidades son aún escasas.

Estado de riesgo del ciberespacio

El ciberespacio específico de la India comparte con el ciberespacio global la categorización de las amenazas a las que está expuesto pero difiere en cuanto a las motivaciones de las mismas.

La India no dispone de un conocimiento de cibersituación fiable y actualizado de su ciberespacio, el del resto de naciones, el del enemigo y cualquier otro que genere interés. Por tanto, es difícil que el gobierno indio pueda planear, dirigir y gestionar su ciberseguridad. Este hecho, sin duda, es conocido y aprovechado por sus enemigos para atacar e infiltrarse en el ciberespacio indio casi sin oposición.

La India es víctima de múltiples ciberataques patrocinados por Pakistán y China. Las relaciones entre India y Pakistán, desde la independencia de esta última de la India en 1947, se caracterizan por una alternancia entre periodos de conflictos armados y 'tensa paz'. La disputa por la región de Jammu y Cachemira y el supuesto patrocinio del gobierno pakistaní al proselitismo musulmán sobre las clases más bajas del hinduismo marcan las tensas relaciones entre ambos países. Desde el punto de vista cibernético, ninguno de los dos países ejerce una supremacía clara sobre el otro. Los ciberataques sobre las redes gubernamentales, principalmente diri-

gidos a los ministerios de Defensa, Interior y Asuntos Exteriores, con el objeto de obtener información sobre los planes nucleares y armamentísticos de ambos países son continuos pero con escaso éxito. Del mismo modo, la mayoría de los ciberataques a los que se someten India y Pakistán son de perfil bajo, perpetrados por grupos de *hackers* especializados en ataques de DDoS o *defacement* sobre webs del gobierno, partidos políticos y grupos religiosos.

Respecto a la relación entre India y China, el Tibet y la territorialidad de pequeñas áreas fronterizas de las regiones de Uttar-Anchal e Himachal-Pradesh marcan las complejas relaciones entre ambos países. En este caso, la supremacía cibernética china es incuestionable, lo que es aprovechado para atacar e infiltrase de manera masiva y continuada en las redes gubernamentales indias, así como en organizaciones pro-Tibet.

Los ciberataques contra las infraestructuras críticas representan una de las mayores preocupaciones del gobierno indio. La creciente demanda energética del país contrasta con la obsolescencia y vulnerabilidad de la infraestructura TIC de los sistemas que deben satisfacer esta demanda. A finales del pasado mes de julio, 600 millones de indios se quedaron sin suministro eléctrico debido a continuos problemas en las principales centrales eléctricas del país. Muchos analistas apuntaron a grupos de *hackers* chinos como causantes de los apagones, aunque no hay evidencias al respecto.

Muchos de los ciberataques que acontecen en el ciberespacio indio son perpetrados por grupos de *hacktivistas*, nacionales e internacionales, patrocinados por países y organizaciones criminales. Tras los atentados terroristas de Mumbai en 2008, el gobierno indio aprobó la *IT Act 2008*, por la que se autorizaba al gobierno a tomar aquellas medidas que considerase oportunas para evitar actividades delictivas a través de Internet. Recientemente, invocando la *IT Act*, el gobierno indio ordenó a los proveedores de telefonía móvil de la región de Assam, al noreste del país, que deshabilitasen temporalmente el servicio de SMS con el objetivo de frenar el éxodo de 50.000 bodos (minoría étnica asentada mayoritariamente en la región de Assam) atemorizados supuestamente, vía SMS, por la comunidad musulmana pro-Bangladesh de Assam.

Además, la fuerte rivalidad entre los dos grandes partidos políticos de la India, el Partido del Congreso (actualmente en el gobierno y defensor de la laicidad del país) y el Partido del Pueblo Indio (defensor de la *hindutva*, es decir, la homogeneidad racial y religiosa entorno al hinduismo), está transportándose al ciberespacio. Ambos partidos políticos hacen uso del ciberespacio para fines propagandísticos, lo que está provocando la radicalización de sus discursos y la proliferación de conflictos regionales que enfrentan a las comunidades hindú y musulmana del país en las regiones fronterizas con Pakistán de Guyarat, Rajastan y Punyab.

Liderazgo y política firme

Pero: ¿Cómo debe afrontar la India el futuro de su ciberseguridad?

El sector privado, la comunidad educativa y los principales *think tanks* de la India reclaman al gobierno que asuma el liderazgo y desarrolle una política firme y efectiva en materia de ciberseguridad. Esta política deberá tener como objetivo proporcionar un ciberespacio seguro y generar una cultura de ciberseguridad que posibilite la prosperidad social, cultural y económica de la India, así como su seguridad y defensa.

El gobierno indio deberá crear un sistema nacional de ciberseguridad, es decir, un conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de su ciberseguridad. Los principales expertos del país defienden la creación de este sistema a partir de la integración y coordinación de los organismos ya existentes. El National Information Board (NIB), por competencias y medios, debería asumir el rol de órgano central del sistema. Del mismo modo, este sistema deberá sustentarse sobre un marco legislativo, una metodología de trabajo común para todos los actores de la ciberseguridad india y una profunda modernización de la infraestructura TIC del país.

El sistema indio de ciberseguridad deberá proporcionar al gobierno indio un conjunto de capacidades y recursos que posibiliten: 1) disponer de un conocimiento de cibersituación fiable y actualizado con el fin de afrontar los riesgos expuestos a lo largo del presente artículo, así como lo que surjan en el futuro; 2) disponer de unos mecanismos ágiles para la compartición de información entre el gobierno, fuerzas armadas, agencias de inteligencia y el resto de actores involucrados en la ciberseguridad del país; 3) mejorar y fortalecer el marco de colaboración público-privada; y 4) centralizar y optimizar las políticas en I+D+i.

La seguridad del ciberespacio indio no es una tarea exclusiva del gobierno y la sociedad india. El carácter global del ciberespacio hace necesaria una estrecha colaboración con la comunidad internacional. Para ello, la India deberá actualizar y renovar los acuerdos en materia de ciberseguridad con otros países. En la actualidad, dispone de un acuerdo de colaboración con los Estados Unidos, el *US-India Cybersecurity Memoradum of Understanding*. Además, el gobierno indio deberá trabajar para alcanzar acuerdos de colaboración similares con el resto de sus aliados.

Desde el punto educativo, se deberá frenar la fuga de talentos nacionales hacia Estados unidos y Europa. Para ello, será necesario aumentar los recursos técnicos y económicos destinados a los IIT, aumentar y fomentar la inversión en I+D+i y mejorar la colaboración público-privada en materia de ciberseguridad.

La ciberconcienciación de la sociedad india es una tarea esencial. Las competencias en esta materia deberán ser asumidas por el gobierno central con el objeto de desarrollar un ambicioso plan de ciberconcienciación temprana.

El gobierno indio deberá trabajar para mejorar la resiliencia nacional respecto de la amenaza cibernética y crear y fomentar una cultura de ciberseguridad. En definitiva, el futuro social, político y económico de la India, así como su seguridad y defensa, está inexorablemente ligado al ciberespacio. En la actualidad, la India está muy lejos de poder afrontar los innumerables riesgos que el ciberespacio le plantea. ■