ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

37/2022 25 de mayo de 2022

Javier Fernández Aparicio

Ciberseguridad en la India: bilateralidad y transformación

Ciberseguridad en la India: bilateralidad y transformación

Resumen:

Con el inicio de la crisis de la pandemia, a principios de 2020, que supuso el aumento cuantitativo del uso de Internet y sus aplicaciones, más los retos en ciberseguridad que esto conlleva, incluyendo ataques a infraestructuras críticas, la India se enfrenta a la necesidad de actualizar su *Política Nacional de Ciberseguridad*, que data de 2013, desarrollando una estrategia en la prevención de amenazas desde el ciberespacio. Todo ello, en unos momentos en los que el gobierno del primer ministro Modi se ha esforzado para llegar a acuerdos bilaterales en la materia con terceros países, en contrapeso a la influencia china, tanto en el espacio indopacífico, como a nivel global, incluyendo el ciberespacio, considerado actualmente el quinto dominio en el ámbito bélico. La guerra en Ucrania ha fortalecido esta línea de compromisos internacionales bilaterales, influyendo en su relación en ciberseguridad y tecnología con Rusia. Además, la India en la actualidad es un país productor clave en la creciente industria 4.0 y en toda la economía que se mueve a su alrededor.

Palabras clave:

India, ciberseguridad, ciberespacio, China, Indopacífico, Rusia.

Cybersecurity in India: bilaterality and transformation

Abstract:

With the onset of the pandemic crisis in early 2020, which brought about a quantitative increase in the use of the Internet and its applications, plus the cybersecurity challenges that this entails, including attacks on critical infrastructure, India is facing the need to update its National Cybersecurity Policy, which dates back to 2013, developing a strategy to prevent threats from cyberspace. All this, at a time when Prime Minister Modi's government has made an effort to reach bilateral agreements on the matter with third countries, in counterweight to Chinese influence, both in the Indo-Pacific space and globally, including cyberspace, currently considered the fifth domain in the field of warfare. The war in Ukraine has strengthened this line of bilateral international commitments, influencing its cybersecurity and technology relationship with Russia. In addition, India is currently a key producer country in the growing industry 4.0 and in the entire economy that moves around it.

Keywords:

India, Cybersecurity, Cyberspace, China, Indo-Pacific, Russia

Cómo citar este documento:

FERNÁNDEZ APARICIO, Javier. *Ciberseguridad en la India: bilateralidad y transformación*. Documento de Análisis IEEE 37/2022. https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA37_2022_JAVFER_India.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

Con el impacto de la pandemia COVID y los acontecimientos en Ucrania, la posición geoestratégica de potencias como China e India es analizada a nivel global por su importancia más allá del espacio indopacífico, donde ambos países juegan un rol clave que indudablemente tiene su continuidad en el orden mundial. Las posiciones de cara al exterior de la India y China reflejan su propia relación, dos gigantescas esferas de poder político, económico, militar y cibernético que se encuentran frente a frente. Recordemos que hay una vecindad estrecha, marcada por una frontera común de cerca de 4.000 kilómetros, la conocida *Line of Actual Control* (LAC), incluyendo la conflictiva región de Cachemira. Desde hace décadas se han producido incidentes fronterizos entre la India y China, siendo en los últimos años de cierta gravedad, como el ocurrido el 15 de junio de 2020 en la región de Aksai Chin, que se tradujo en militares de ambos países muertos, y que dio lugar, según fuentes indias, a una serie de ciberataques y campañas de desinformación desde China y Pakistán[1].

Así, el veloz ascenso de la presencia china en el marco indopacífico, reflejo del global, ha provocado una activación y mayor cercanía, aunque todavía lejos de una colaboración estrecha, de los países que forman el Quad, el foro de seguridad formado por Estados Unidos, Japón, Australia y la propia India[2]. También, durante 2015-2016 se apreció un acercamiento bilateral indo-estadounidense, buscándose así un contrapeso a la preeminencia china en la zona, lo que se simboliza en materia comercial[3] y en una cooperación en seguridad. En la actualidad se negocia un contrato para aprovisionar de cazas F-18 al proyectado portaaviones indio *INS Vikrant*[4]. Dentro de estas capacidades militares y de defensa, el papel de la ciberseguridad es primordial, configurándose también una cooperación entre la India y Estados Unidos en este terreno.

[1] NANDINI, Navashree. India-China Faceoff: Chinese mouthpiece silent on casualties; its journalists say 5 dead (republicworld.com) 16/6/2020 (consultado 28/04/2022). Según un funcionario del gobierno, activistas chinos y paquistaníes habían comenzado campañas en las redes sociales para supuestamente difundir información errónea contra la India. En RAIBAGI, Kashyap. India's Current Cybersecurity Policy & How It Was Impacted By COVID (analyticsindiamag.com) 5/12/2020 (consultado 11/5/2022).

[2] HERRERA PILAR, Mikel. *El Quad en la era post-COVID: más allá del desafío chino*. Documento de Opinión IEEE 102/2021. http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO102_2021_MIKHER_Quad.pdf (consultado 26/4/2022).

[3] JUSTER, Kenneth I. Es hora de que Estados Unidos e India hablen de comercio | Asuntos exteriores (foreignaffairs.com) 14/4/2022 (consultado 26/4/2022).

[4] La India se debate entre cazas F-18 y Rafale para su nuevo portaaviones (infodefensa.com) 18/4/2022 (consultado 26/4/2022).

No hay que olvidar tampoco otro factor clave, este más interno y avalado por los estudios estadísticos, como es el creciente uso masivo e importancia de la red en toda la India, impulsado desde el Gobierno como parte de la modernización del país. Se trata de un fenómeno acelerado desde 2020.

La ciberseguridad en la India

El impacto de la India a nivel mundial en la utilización de Internet es tan significativo, que en este de por sí poblado país de 1.400 millones de habitantes, sus actuales 658 millones de usuarios de la red la sitúan como el segundo país del mundo, solo por detrás de China, con un millardo, y doblando los más de 300 millones de Estados Unidos.

Otra prueba de la magnitud del empleo de Internet en la India es que, de esos 658 millones de usuarios, 467 también lo son de las redes sociales, lo que equivale a decir que un 33,4 % de la población total india, en la práctica una tercera parte, las utiliza y está conectada. Sin embargo, hay diferencias sustanciales en esta demanda de Internet, así como una brecha digital, puesto que aquella está centrada en las grandes urbes, cuya población, no obstante, es el 36 % del total respecto a la rural, que representa el 65 % a principios de 2022[5].

Precisamente, para paliar esta brecha digital, en 2015 el Gobierno puso en marcha el proyecto *Digital India*, una iniciativa con múltiples implicados, desde el sector económico al tecnológico y que exige fuertes inversiones y es prioritario, tal y como demuestra su dependencia directa del propio primer ministro, Narendra Modi. *Digital India* establecía tres objetivos en materia cibernética a nivel nacional[6]:

1. Creación de una infraestructura digital de servicios públicos, llegando a todo el país.
2. Constitución de un marco legal de gobernanza y ciberseguridad de estos servicios.
3. Empoderamiento digital de los ciudadanos y empresas indias, accediendo a la red desde cualquier parte.

[5] Datos de enero de 2022. Digital 2022: India — DataReportal – Global Digital Insights (consultado 20/4/2022).
[6] Áreas de Visión y Visión | programa India Digital | Ministerio de Electrónica y Tecnología de la Información (MeitY) Gobierno de la India (digitalindia.gov.in) (consultado 24/4/2022).

En la práctica, *Digital India* suponía el desarrollo de diversos proyectos secundarios para avanzar en la digitalización de la Administración, incluyendo lo concerniente a la defensa y seguridad, junto a la conexión de las zonas rurales mediante fibra óptica. Estos proyectos se abrieron a la inversión privada para su implantación. Conectar todos los enclaves de la India supone un desembolso y esfuerzo titánicos. Al respecto, *Bharat Net* es el principal plan elaborado desde el Departamento de Tecnología Electrónica y de Información, dentro del Ministerio de Comunicación y Tecnología de la Información, responsable en gran medida de *Digital India*. El plan tiene la finalidad de llegar a todos los Gram panchayats del país, la institución básica municipal de las casi 625.000 aldeas de la India. A finales de febrero de 2022, *Bharat Net* había contabilizado la instalación de más de 36.000 kilómetros de fibra óptica en todo el país, así como establecido cerca de 105.000 puntos de acceso wifi[7].

Una de las consecuencias de esta extensión en el acceso rápido a Internet, desde la Administración hasta los particulares, con una lógica multiplicación de descargas, aplicaciones y servicios, es que la India también debe atender a un vasto ciberespacio desde una óptica de seguridad.

Según un estudio de la firma Comparitech, en 2019, la India ocupaba el puesto número 15 dentro de un *ranking* de países con poca seguridad cibernética. La conclusión del informe es muy clara: la India se sitúa como uno de los países menos ciberseguros del mundo, en contraposición a su peso dentro del concierto internacional y de su importancia en la economía de la industria 4.0[8]. Desde el Gobierno, se han hecho esfuerzos progresivos al respecto durante los tres últimos años, al ser el ciberespacio una necesidad ineludible de la seguridad nacional del país.

La política nacional india en ciberseguridad

Hay cierta indefinición en cuanto a la normativa y los organismos competentes en materia de ciberseguridad en la India. Ello tiene como principales consecuencias el solapamiento de atribuciones y una petición casi unánime de la sociedad india de una mayor transparencia y centralidad en este terreno, en especial en lo tocante a la protección de

[7] Según las cifras estimadas por el Ministerio de Electrónica y Tecnología de la Información, recogidos en *Vikaspedia*, la base de datos de información mantenida por el Gobierno de India desde 2014. Bharat Net — Vikaspedia (consultado 20/4/2022).

[8] India ranks among the worst in the world for cybersecurity, *FRPT- Software Snapshot*. Febrero 2019:2. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=135716406&lang=es&site=ehost-live (consultado 9/5/2022).

datos e intimidad de las empresas y personas, ya que han salido a la luz casos de ciberespionaje[9].

El marco jurídico indio se remonta a la Ley de Telégrafos de 1885, que permitía a las autoridades gubernamentales acceder a comunicaciones privadas y datos de identificación, aunque en circunstancias determinadas y siempre en interés teórico de la seguridad nacional. La política india específica en el ámbito de la ciberseguridad se retrotrae al año 2000, cuando se promulgó la *Information Technology Act* (conocida por sus siglas como *IT Act*), que regulaba las transacciones electrónicas y las comunicaciones digitales, haciendo hincapié en la protección de datos y en los, por entonces incipientes, ciberdelitos. La ley establecía su revisión periódica por parte de una comisión de expertos en diferentes campos y tuvo diversas adendas, siendo la última en 2011[10].

Desde 2006, este comité permanente de la *IT Act* venía pidiendo una nueva legislación para gobernar el ciberespacio, abordando los fenómenos del ciberterrorismo, la ciberdelincuencia, los delitos cibernéticos transfronterizos e introduciendo el término de «infraestructura de información crítica» para definir por primera vez un recurso cibernético de impacto para la seguridad nacional[11].

Reconociendo esta necesidad de una ciberseguridad cada vez más urgente, además de responder a las acusaciones de espionaje de la Agencia Nacional de Seguridad norteamericana a diversas personalidades del gobierno indio[12], el entonces Ministerio de Comunicación y Tecnología de la Información redactó en julio de 2013 la Política de Ciberseguridad Nacional india (PCNSI), con un objetivo fundamental: conseguir un ciberespacio seguro en la India, tanto para el ámbito institucional como para el privado, es decir, para todas las operaciones en la red de ciudadanos y empresas indias.

El documento también recogía otras misiones como era la de proteger las infraestructuras críticas del país, prevenir y responder a las amenazas cibernéticas del exterior y fomentar la investigación y desarrollo de tecnologías de seguridad propias, para no depender así de países o compañías extranjeras. Para ello, se creaba un llamado «ecosistema nacional» para velar por la ciberseguridad, designándose a un equipo de respuesta rápida a las posibles amenazas del ciberespacio bajo el paraguas

[9] BAJORIA, Jayshree. RAW: India's External Intelligence Agency | Council on Foreign Relations (cfr.org) 7/11/2008 (consultado 9/5/2022).
[10] SUBRAMANIAN, Aditi. Cybersecurity Report 2022 India (iclg.com).
[11] Cyber security framework under the IT Act in India | Ikigai Law 23/6/2020 (consultado 5/5/2022).
[12] HARRIS, Shane. What Was Edward Snowden Doing in India? – Foreign Policy 13/1/2014 (consultado 5/5/2022).

de un nuevo organismo, el Centro Nacional de Protección de Infraestructura de Información Crítica (NCIIPC).

Además, se proyectaba un mando cibernético único para las Fuerzas Armadas indias, aunque no se definía ni la ubicación ni la estructura jerárquica del mismo[13].

En 2019, un informe sobre el estado de la seguridad nacional encargado por el histórico partido indio Congreso Nacional, rival del Bharatiya Janata del primer ministro Modi, al prestigioso y retirado teniente general Deependra Singh Hooda, defendía una revisión global de la política en ciberseguridad del país, junto a una mayor inversión en la misma. El documento concluía que la India necesitaba un mando cibernético único y avisaba de que la tecnología del país no estaba preparada para hacer frente a los conflictos del ciberespacio[14].

Con el paso del tiempo, como consecuencia de la pandemia y del ya citado incremento cuantitativo del uso de Internet y sus riesgos, desde más sectores se ha venido pidiendo una actualización de la Política Nacional de Ciberseguridad. Aunque existen algunos proyectos cooperativos entre el Ministerio de Electrónica y Tecnología de la Información y el Ministerio de Información y Radiodifusión, más bien estaríamos ante diversas directrices o declaraciones de intenciones en la materia, sin mayor consecuencia práctica[15].

En estricta materia de defensa del ciberespacio, la Política Nacional de Ciberseguridad india de 2013 contiene directrices para proteger de amenazas a todos los usuarios indios: pequeños y medianos negocios, más los ciudadanos. También se promueve la concienciación de la sociedad sobre la importancia de la ciberseguridad; se aboga por un entorno jurídico para perseguir los ciberdelitos, entorno aún no perfilado, y se recomienda la elaboración de planes de protección de redes e infraestructuras críticas. Finalmente, se insta a la investigación tecnológica propia, para no depender de un actor externo y, muy importante, solicita acuerdos y tratados bilaterales en materia de ciberseguridad con terceros países, lo que sí se ha desarrollado[16].

[13] SANJIV, Tomar. National Cyber Security Policy 2013: An Assessment | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in) 24/4/2013 (consultado 29/4/2022).
[14] PANDEY, Shreya. The Hooda document : expanding the contours of 'national security' (ipleaders.in) 17/8/2020 (consultado 12/5/2022).
[15] Data Security Council of India. National Cyber Security Strategy 2020 DSCI submission.pdf (consultado 11/5/2022).
[16] RAIBAGI, Kashyap. *Op. cit.*

La infraestructura india en ciberseguridad

India cuenta con diversos organismos nacionales que velan por el marco de la ciberseguridad en las infraestructuras críticas, públicas y privadas. Según sus propias declaraciones, para el primer ministro Modi, la ciberseguridad de las mismas es una prioridad, no solo desde un punto militar o bélico, sino porque las ciberamenazas tienen el potencial de afectar gravemente a toda la sociedad, la economía y, en definitiva, al desarrollo del país[17].

Hay cierta indefinición de competencias entre los principales organismos que velan por el ciberespacio indio, donde cabe citar como principales centros:

- El **National Technical Research Organisation (NRTO)**. Es la principal institución en el campo de la ciberseguridad y la recopilación de datos de inteligencia, dependiendo desde 2004 del consejero de Seguridad Nacional de la Oficina del Primer Ministro, cuando aún se llamaba National Technical Facilities Organisation. Obtiene información mediante diversas fuentes en inteligencia, captación y recopilación de datos, criptografía, detección y vigilancia espacial, inteligencia satelital, monitoreo de Internet y el desarrollo de *software* en materia de ciberseguridad. Transmite los datos a la Administración india, incluyendo a las Fuerzas Armadas, aunque orgánicamente la NRTO no tenga relación con ellas[18].

  La NTRO incluye en su organigrama, a su vez, a dos agencias con competencias en ciberseguridad. Una es el **National Critical Information Infraestructure Protection Centre (NCIIPC)**, que desde enero de 2014 facilita protección específica de las infraestructuras críticas ante ataques cibernéticos, incluyendo transporte, telecomunicaciones, finanzas, instalaciones energéticas e instituciones del gobierno, siendo su principal misión prevenir «el acceso no autorizado, la modificación, uso o

[17] BHARDWAJ, Ananya. India to get new, 'robust' cyber security policy soon, says PM Modi (theprint.in) 15/4/2022 (consultado 11/5/2022).

[18] Según declaraciones del ex analista de la NSA, Edward Snowden, esta agencia de seguridad estadounidense colabora activamente con la NRTO, en el marco de la SIGINT Seniors Pacific (SSPAC), una plataforma internacional antiterrorista formada por Estados Unidos, Australia, Canadá, Francia, India, Corea del Sur, Nueva Zelanda, Singapur, Tailandia y Reino Unido. BARUAH, Sanjib Kr. 'India joined US-led top secret alliance in 2008' (asianage.com) 10/3/2018 (consultado 21/4/2022).

divulgación no autorizada, interrupción o incapacitación» de información relevante de dichas infraestructuras críticas[19].

El segundo centro bajo autoridad de la NTRO es el **National Institute of Cryptology Research and Development (NICRD)**, un organismo de investigación criptológica que data de 2007 y cuya función principal es el cifrado seguro para las aplicaciones cibernéticas en las infraestructuras críticas, tanto de carácter público como privadas.

- El **National Cyber Coordination Centre (NCCC)** es una agencia creada en 2014, pues se contemplaba en la *Política Nacional de Ciberseguridad*, de un año antes, como parte del Ministerio del Interior. El NCCC se encarga de concienciar a la sociedad india sobre la importancia de la ciberseguridad y coordina el trabajo de varias agencias estatales en este campo. Como la NTRO, también monitorizar la Red, pues se constituye como teórico «primer muro de contención» de las amenazas cibernéticas, y elabora estrategias de prevención de ciberataques. Está bajo la autoridad de un coordinador nacional en ciberseguridad. Al no tener una regulación específica, la NCCC ha sido acusada de ciberespionaje masivo a ciudadanos indios[20].
- El **CERT-In** es un departamento dentro del Ministerio de Tecnología de la Información y Electrónica existente desde 2003 y encargado, por ejemplo, del proyecto *Digital India*. Emite instrucciones para bloquear sitios webs maliciosos, pues su objetivo es obtener un ciberespacio seguro, pero enfocado sobre todo a proveedores privados de servicios de Internet y empresas del país, a las que trata de prevenir y defender de ciberataques[21].
- El **Research and Analysis Wing** (RAW) es la principal agencia de inteligencia india centrada en el análisis de la política exterior en relación con la seguridad nacional, en especial lo tocante a Pakistán y China. Por ello, lógicamente, los temas relacionados con la ciberseguridad han adquirido mucha importancia y prueba de ello es que posee una sección propia para asuntos tecnológicos. La relevancia de la RAW, creada en 1968 pero cuyas raíces se pueden rastrear incluso a la época anterior a la

[19] Centro Nacional de Protección de la Infraestructura de Información Crítica, Gobierno de la India (nciipc.gov.in) (consultado 25/4/2022).
[20] NIGAM, Aditiya. Hacking India's Democracy – From Monitoring Metadata to Spying Real Time: C.P. Geevan | KAFILA – COLLECTIVE EXPLORATIONS SINCE 2006 26/7/2021 (consultado 10/5/2022).
[21] Indian - Computer Emergency Response Team (cert-in.org.in) (consultado 25/4/2022).

independencia, hace que, como la NTRO, dependa de manera directa de la Oficina del Primer Ministro[22].

Incidentes de ciberseguridad en la India

Lo primero a citar es el aumento de los ciberdelitos en la India durante 2021, que incluye serias acusaciones hacia la actividad de diferentes agencias gubernamentales, dedicadas a la ciberseguridad, de haber monitorizado y espiado dispositivos de miles de ciudadanos indios. En 2018 el Ministerio del Interior aprobó una directiva que autorizaba a interceptar cualquier información recibida o almacenada en organismos oficiales, incluyendo las fuentes de la Policía y sus ficheros, lo cual llevó a la impugnación de la directiva ante el Tribunal Supremo por parte de una plataforma de ciudadanos, al entender que se violaba claramente el derecho a la intimidad.

La India tampoco ha sido ajena a la polémica por la utilización del *software* israelí *Pegasus.* Algunas fuentes afirman que se ha espiado dispositivos de algunos periodistas y opositores políticos, hoy en día, es una cuestión que sigue en los tribunales[23].

Durante 2021 hubo algún tipo de incidente de ciberseguridad en el 52 % de las grandes corporaciones indias. El mayor de ellos fue la violación de los datos del pasaporte de más de cuatro millones de pasajeros de Air India, al ser hackeado el sistema de un proveedor de datos de la aerolínea, llamado SITA[24]. En otro ciberataque masivo ocurrido en mayo de 2021, revelaron los datos personales de unos 180 millones de clientes de la popular cadena de restauración, Domino's Pizza[25].

También se produjeron incidentes en ciberseguridad en el ámbito público; por ejemplo, los resultados de los test de COVID-19 de miles de ciudadanos se sacaron a la luz sin respeto a la privacidad de aquellos, tras un ciberataque a la web del sistema sanitario indio. En este mismo sentido de divulgación de datos personales, a finales de 2020 hubo otro caso relevante. Se trató de la promulgación, por parte del Ministerio de Agricultura y Bienestar de los Agricultores, de las conocidas como «leyes de la agricultura», cuyo fin

[22] Ala de Investigación y Análisis [RAW] - Agencias de Inteligencia de la India (globalsecurity.org) (consultado 25/4/2022).
[23] DHILLON, Amrit & SAFI, Michael. Indian supreme court orders inquiry into state's use of Pegasus spyware | India | The Guardian 27/10/2022 (consultado 10/5/2022).
[24] SATIJA, R. Cyber-Attack on Air India Led to Data Leak of 4.5 Million Fliers, *Bloomberg.com*, *[s. l.]*. 2021. https://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=150446593&lang=es&site=ehost-live (consultado 10/5/2022).
[25] VACHHATANI, Jitesh. Domino's India faces cyber attack; data of 18 cr orders, including personal info, leaked (republicworld.com) 23/5/2021 (consultado 11/5/2022).

teórico era modernizar los procesos agrícolas del país, incluyendo la compraventa rápida de productos a través de la red. Este procedimiento era contestado por parte de la población rural, debido a la imposibilidad de acceso a Internet o la falta de competencias digitales. Desde el Ministerio se incluía un formulario *online* para acceder a determinadas ayudas, en donde era preciso especificar los datos personales de los peticionarios. Dicho formulario contenía un enlace que descargaba un *ransomware* que inhabilitaba los equipos de los peticionarios, a los que además les aparecía un mensaje pidiendo un rescate para restaurar los equipos, al tiempo que se leía un manifiesto contrario a las citadas «leyes de la agricultura» [26].

Otro riesgo cibernético es la inversión en el criptomercado indio, que le ha convertido en uno de los centros mundiales de la criptomoneda en 2021. Este creciente mercado de la India es un gran atractivo para inversores extranjeros, pero también para las actividades fraudulentas, ya sean por los pagos de actividades delictivas, como las de un hacker desde Bangladés que había conseguido obtener información sensible de portales gubernamentales indios, caso aún abierto, incluyendo a algunos cargos políticos indios implicados[27].

Ante las amenazas de la ciberdelincuencia en este campo, el Gobierno diseña nuevas disposiciones para estabilizar la actividad de este mercado de criptomonedas, en especial desde el punto de vista fiscal y también respecto a los *tokens* digitales, tratando de reducir este comercio altamente especulativo y, además, aumentando por esta vía los ingresos públicos[28].

Cooperación internacional india en ciberseguridad

En el contexto internacional, desde 2015 la India y Estados Unidos reforzaron su colaboración en la lucha contra el crimen cibernético, inaugurando una política de acuerdos bilaterales internacionales de la India en la materia, que han dado lugar a un marco común de cooperación en materia cibernética[29]. En el verano de 2016 se firmaron unas directrices en Nueva Delhi para compartir información en tiempo real y cooperar en

[26] SUBRAMANIAM, Aditi. *Op. cit.,* p. 8.
[27] BANERJEE, Swagata. Priyank Kharge targets BJP over alleged Bitcoin Scam: 'Why was Hacker granted bail?' (republicworld.com) 10/11/2021 (consultado 11/5/2022).
[28] Investment in Indian crypto market will rise - Oxford Analytica Daily Brief (oxan.com) 7/4/2022 (consultado 21/4/2022).
[29] Joint Statement—2016 United States-India Cyber Dialogue, *Daily Compilation of Presidential Documents*, *[s. l.]*. 2016, p. 1-2. https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=118809843&lang=es&site=ehost-live (consultado 11/5/2022).

la investigación conjunta, incluyendo productos en ciberseguridad, con un diálogo fluido entre los organismos responsables de cada país[30]. Tanto Estados Unidos como la India parecen tener un objetivo común en el horizonte: China. Hay que recordar que, a la prohibición en Estados Unidos, en 2020, de importar *hardware* y aplicaciones chinas, siguió el establecimiento de la misma restricción en otros países, entre ellos la India, exponente de una guerra digital y comercial entre ambos países[31].

Este tipo de entendimiento bilateral en materia de ciberseguridad se ha repetido con otros países. En el año 2018, los primeros ministros israelíes e indio sellaron, entre otros acuerdos, uno de cooperación en materia de ciberseguridad. Un año antes, se firmó un memorando de entendimiento en ciberseguridad entre India y España, aprovechando para ello la visita del primer ministro Modi a nuestro país en mayo de 2017. Esta hoja de ruta supone el germen de una alianza indo-española en la materia, donde también cabe la cooperación tecnológica[32].

En la región del Indopacífico, en materia de ciberseguridad se estrecharon los lazos entre la India y Australia, con una asociación estratégica bilateral en 2020, donde una de las prioridades era la ciberseguridad común de ambos países. Además, también se buscó la asociación de empresas tecnológicas indo-australianas para abordar la seguridad cibernética y la economía pareja desde una perspectiva conjunta, poniendo también el foco en las posibles amenazas en este campo llegadas desde China[33].

En octubre de 2021, altos representantes de 25 países, incluyendo a los países del sudeste asiático agrupados en la ASEAN, Estados Unidos, la Unión Europea e India, se reunieron en una sesión virtual para tomar medidas conjuntas contra el *ransomware*, reconociendo así que esta práctica cibercriminal es una de las amenazas más importantes a escala global. La reunión estableció un principio de acuerdo para involucrar tanto al sector público como al privado de todos los países, además de consensuar la necesidad de concienciar a la sociedad sobre este peligro cibernético, junto a otros, y la necesidad de protegerse[34].

[30] Framework for the U.S.-India Cyber Relationship - U.S. Embassy & Consulates in India (usembassy.gov) 30/8/2016 (consultado 10/5/2022).
[31] ALDAMA, Zigor. Primero EEUU y ahora India: la guerra digital contra China que está rompiendo internet (elconfidencial.com) 3/7/2020 (consultado 11/5/2022).
[32] Fundación Consejo España-India. Documento 5. Ciencia, tecnología e innovación, *Informe España-India 2020*. Madrid, 2020. http://www.spain-india.org/files/documentos/2021_DOC_5_INFORME_ESPANA_INDIA_(3).pdf (consultado 25/4/2022).
[33] PANKAJ, Jha & STAR, Shaun. India–Australia. Defining New Horizons of Engagement, *Strategic Analysis*, 45:5. 2021, pp. 411-430. DOI: 10.1080/09700161.2021.1965344 (consultado 10/5/2022).
[34] Significance of India's Act East Policy and Engagement with ASEAN | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in) 7/12/2018 (consultado 12/5/2022).

Impacto del conflicto de Ucrania en la relación con Rusia y China

El actual conflicto en Ucrania y la posición ambigua de la India respecto a Rusia ha generado interrogantes (pues se abstuvo de condenar la agresión rusa en la resolución al respecto de Naciones Unidas) que también se trasladan al campo de la ciberseguridad. En septiembre de 2021, ambos países celebraron sendas reuniones para acordar una política conjunta, al estilo de otros acuerdos bilaterales, y perseguir los delitos en el ciberespacio que les afectasen comúnmente[35].

Aunque esta posición india de cierta ambigüedad pueda parecer un elemento de disensión, al menos dentro del grupo de países del Quad, lo más probable es que se trate de una discrepancia mínima, respecto al otro gran reto que supone la hegemonía china[36].

Desde hace décadas, Rusia e India son socios cercanos para asegurar sus intereses mutuos, tanto en un entorno regional como global. Nueva Delhi recientemente permitió a Moscú invertir en fondos de deuda pública india, importó más petróleo ruso y hoy es posible que esté considerando un sistema de pago alternativo a sus importaciones y exportaciones, que eludan las sanciones internacionales a Rusia por la invasión de Ucrania[37]. Por su parte, las empresas indias participan en el ecosistema tecnológico ruso y en la actualidad el éxodo masivo de empresas tecnológicas occidentales desde Rusia, abre aún más una puerta para expandir esta participación india en otros mercados, como, por ejemplo, los segmentos de computación en la nube, aprovechando que Google Cloud y empresas similares han suspendido sus servicios, o las actividades comerciales de

[35] Russia, India ready to cooperate on cybersecurity, *Russia & CIS Military Newswire.* 7/9/2021. https://www.proquest.com/wire-feeds/russia-india-ready-cooperate-on-cybersecurity/docview/2569687422/se-2?accountid=32797 (consultado 11/5/2022).
[36] CHANDRASHEKHAR OAK, Niranjan. Quad and the Ukrainian Crisis (idsa.in), *Issue Brief MP-IDSA.* 22/3/2022 (consultado 26/4/2022).
[37] IVASHENTSOV, Gleb A. Russia-India: Strategic Partnership, Not Alliance, *Strategic Analysis*. 2020. DOI: 10.1080/09700161.2022.2039579 (consultado 12/5/2022).

teléfonos inteligentes. Con todo, la actual situación es muy compleja y cambiante en esta relación tecnológica y comercial indo-rusa[38].

Respecto a China, como hemos expuesto, la India tiene una estrategia para fortalecer la seguridad cibernética del país frente a las supuestas intrusiones chinas que, según algunas fuentes, podían haber intentado afectar a varias infraestructuras críticas, como la Bolsa o el suministro eléctrico[39].

La relación tecnológica entre ambos países ha dado un giro considerable, también como consecuencia del intento indio para exportar sus productos y servicios en relación con la industria 4.0, y no depender al respecto del mercado extranjero, en especial de China.

Antes de 2020 y durante el lustro anterior, China había invertido en el sector tecnológico indio de forma decidida como antesala de su proyecto *Belt and Road Initiative* (BRI), la estrategia de inversión en infraestructuras con capital chino en diversos países extranjeros, incluyendo los del Indopacífico, creada en 2013[40]. Hasta ahora, se calcula que casi 4.000 millones de dólares han sido invertidos por entidades chinas en empresas tecnológicas, aplicaciones y *start-ups* desarrolladas en India[41].

En 2017, aparecieron las primeras tensiones entre los dos gigantes, a cuenta de la inversión china en el corredor económico de Pakistán a través de la disputada Cachemira, lo que supuso la negativa india a incluir un representante propio en el foro del BRI, una auténtica muestra del rechazo del Gobierno de Modi hacia esta política expansiva china en una región siempre inestable y conflictiva[42]. El nuevo panorama geoestratégico abierto tras la crisis de la pandemia y la guerra en Ucrania han tensado aún más la relación indo-china, como vimos al principio, incluyendo algunos incidentes fronterizos, una reticencia compartida que también tiene su repercusión en el sector tecnológico, comercial y, por supuesto, las amenazas del ciberespacio.

---

[38] Western sanctions alter Russia's technology strategy - Oxford Analytica Daily Brief (oxan.com) 12/4/2022 (consultado 21/4/2022).

[39] CHAUDHARY, A. China Hacking Concern Revives India Focus on Cybersecurity Plan, *Bloomberg.com*, [s. l.]. 2021. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=149132917&lang=es&site=ehost-live (consultado 12/5/2022).

[40] Desde mayo de 2018, el Banco Mundial se ha ocupado en monitorizar el BRI con estándares respecto al comercio, inversión, deuda, adquisiciones, impacto en el medio ambiente, reducción de la pobreza y estado de las infraestructuras globales. En RUTA, Michele. Belt and Road Initiative, *World Bank Brief.* 29/3/2018. https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative?cid=EXT_WBEmailShare_EXT (consultado 28/4/2022).

[41] BHANDARI, Amit; AGARWAL, Aashna & FERNANDES, Blaise. Chinese investments in India - CIAO (ciaonet.org), *Gateway House: Indian Council on Global Relations,* Report No. 3, Map No. 10. February 2020 (consultado 28/4/2022).

[42] DARSHANA, M. Baruah. India's Answer to the Belt and Road: A Road Map for South Asia - Carnegie India - Carnegie Endowment for International Peace 8/2018 (consultado 28/4/2022).

Conclusiones

En materia de ciberseguridad, la India tiene pendiente revisar su estrategia nacional de 2013, para adecuarla a los nuevos tiempos en la materia. Con cientos de millones de usuarios navegando en el ciberespacio, tanto en el ámbito público como en el privado, dicha revisión parece una prioridad ineludible a corto plazo.

Con todo, la India compromete cada vez más recursos en ciberseguridad, ciberespionaje y en prevenir amenazas del ciberespacio en infraestructuras críticas, en ocasiones aprovechando un limbo jurídico en lo concerniente a la protección de datos e intimidad de sus ciudadanos.

No obstante, la existencia de diversos organismos en materia de ciberseguridad, no hay un mando central y unitario que los coordine, aunque destaque la National Technical Research Organitation, por sus competencias.

En el panorama internacional, desde 2016 existe una sólida colaboración con Estados Unidos en materia de ciberseguridad, seguido de una serie de acuerdos bilaterales de la India con diversos países, incluyendo también a Rusia. En el ciberespacio se observa una confrontación con China, reflejo de la pugna de ambos países en el espacio indopacífico y a nivel global. Esos acuerdos bilaterales de la India tienen como objetivo prevenir las ciberamenazas, en primer lugar desde China.

Por último, también hay que tener en cuenta el crecimiento de la industria 4.0 en India, incluyendo a multitud de empresas dedicadas a la fabricación de *hardware* y sus componentes, *software*, aplicaciones, etc., que representan, cada vez más, una parte importante para la economía india, erigida en gran proveedora global y en franca competencia en los mercados internacionales, precisamente frente a China.

Javier Fernández Aparicio
Analista del IEEE