Los desafíos en materia de ciberseguridad en el siglo XXI en las relaciones sino-rusa e indo-rusa

Micaela Capellino[1]
Catalina Virgili[**]

Resumen

Como herramienta fundamental del siglo XXI, el internet ha ganado cada vez más espacio en las agendas de los países. No obstante, también este instrumento ha servido para llevar adelante ataques cibernéticos en el ciberespacio. En tanto, es evidente que con el acelerado avance de las Tecnologías de la Comunicación y la Información (TICs) conjugado con la realidad posterior a la pandemia por el COVID-19, los Estados han hecho mayor foco en la temática de la ciberseguridad.

El triángulo de Rusia, India y China, que se fue consolidando gracias a los periódicos encuentros del foro BRICS, no se ha quedado atrás en esta cuestión. En consecuencia, el presente artículo se propone como objetivo indagar en la forma en que los países de la tríada RIC han abordado los desafíos de la ciberseguridad durante el siglo XXI. Para ello, el trabajo comienza con un breve acercamiento a la cuestión de la ciberseguridad, para luego conocer el abordaje que cada país ha proporcionado a la temática y, por último, indagar si existen programas de cooperación, agendas comunes o estrategias conjuntas entre las partes.

Palabras claves: Ciberseguridad, Rusia, India, China.

The challenges of cybersecurity in the 21st century in sino-russian and indo-russian relations

Abstract

As a crucial tool of the 21st century, the internet has increasingly permeated national agendas. Nonetheless, this tool has also been exploited for carrying out cyber-attacks in cyberspace. It is evident that, with the rapid advancement of Information and Communication Technologies (ICTs) compounded by the post-COVID-19 pandemic reality, states have shifted their focus towards cyber security issues. The trio of Russia, India, and China, solidified through regular meetings within the BRICS forum, has not lagged behind in addressing this matter. Accordingly, this article aims to delve into how the RIC triad countries have tackled the challenges of cyber security in the 21st century. To achieve this objective, the paper commences with a brief overview of cyber security,

[1] Licenciada en Relaciones Internacionales (UNR). Miembro del Grupo de Estudios de Rusia en Rosario (GEЯR). Miembro del Centro de Investigaciones en Política y Economía Internacional de la Facultad de Ciencia Política y Relaciones Internacionales (CIPEI). ORCID: 0009-0009-3634. Correo: cap.mica7@gmail.com

** Estudiante avanzada de la Licenciatura en Relaciones Internacionales (UNR). Miembro del Grupo de Estudios de Rusia en Rosario (GEЯR). ORCID: 0009-0008-9476-9705. Correo: virgilicatalina@gmail.com

then proceeds to examine each country's approach to the issue, and concludes by scrutinizing the presence of cooperation programs, shared agendas, or joint strategies among the involved parties.

Key words: Cybersecurity, Russia, India, China.

TRABAJO RECIBIDO: 18/12/2023 - TRABAJO ACEPTADO: 27/03/2024

Introducción

Es de público conocimiento el hecho de que internet se ha convertido en uno de los instrumentos más importantes en el siglo XXI, en tanto sirve como herramienta para promover nuevas estructuras y espacios de influencia en lo que se denomina la sociedad de la información (Eriksson & Giacomello, 2009, p. 211). En este sentido, con el rápido avance de las Tecnologías de la Comunicación y la Información (TICs) y junto con la pandemia de COVID-19, la ciberseguridad pasó a ocupar un rol primordial en la agenda internacional, de manera acompasada con la intensificación de los ataques cibernéticos a regímenes de seguridad tradicionales que van quedando obsoletos (De Groot, 2023).

En consecuencia, el ciberespacio está en la mira de los gobiernos como próximo espacio a regular de manera internacional. Por lo tanto, un gran conjunto de países se ha mostrado preocupado por desarrollar mayores y mejores controles de este espacio, con el objetivo de establecer leyes que regulen el control del flujo de la información en red y la salvaguardia de sus intereses nacionales (Schreiber, 2019). En este contexto, Rusia, China e India, miembros del conocido triángulo "RIC" no se han quedado atrás. El acrónimo se fue consolidando en el seno de los encuentros a los que los tres países asisten como miembros del foro BRICS, donde cada vez más, han prestado atención a las cuestiones de seguridad internacional para trabajar juntos y hacer frente a las dificultades que se presentan. De hecho, la ciberseguridad comenzó a aparecer como una parte integral de la seguridad de la información de RIC, lo cual influyó de diferentes formas en las regulaciones nacionales (Chislova & Sokolova, 2021).

En este contexto, el presente artículo se propone responder al siguiente interrogante: ¿cómo han abordado los países del RIC los desafíos de la ciberseguridad durante el siglo XXI? De este modo, el trabajo tiene como objetivo situar al subgrupo RIC en el marco del bloque BRICS, para luego realizar un acercamiento a la idea de ciberseguridad y, en tercer lugar, examinar el abordaje que proporciona cada país a esta temática, así como indagar si existe cooperación en la materia.

1. El Triángulo RIC y la ciberseguridad

En la década del 2000, dos artículos escritos por el economista Jim O'Neill, miembro de Goldman Sachs, una firma mundial vinculada a la gestión de inversiones y valores, esbozó el concepto "BRIC" para referirse al potencial que tenían en aquel entonces Brasil, Rusia, India y China, luego de que se sucediera el encuentro de los mandatarios por fuera de la reunión del Grupo de los Ocho (G8) celebrada en San Petersburgo, Rusia, en el año 2008. En este sentido, bajo la idea de O'Neill (2001) de

que estos países pudieran conformar un sólido bloque económico, su objetivo era brindar una orientación a los grandes inversores globales para vincularse con ellos. Dos años más tarde, los líderes se encontraron nuevamente, momento en el cual fue invitada Sudáfrica, reemplazando el acrónimo por "BRICS". Mientras se sucedía el superciclo de las materias primas[2], el ascenso de los países emergentes era inminente. En este sentido, el grupo BRICS se centró en poder aunar sus esfuerzos para resaltar sus voces en la comunidad internacional, a través de alcanzar determinados objetivos como la cooperación económica, el financiamiento para el desarrollo, los intercambios sociales y culturales, la coordinación política, entre otros (Chen et al., 2023).

Sin embargo, debemos decir que los tres países ubicados en el medio del acrónimo BRICS han utilizado el foro para estrechar sus vínculos en distintas materias de cooperación. Es así que se fue consolidando el acrónimo RIC, referido a la relación entre Rusia, India y China. Este subgrupo no es menor, ya que se trata de los tres países principales en la región de Eurasia, dos de ellos con la mayor población mundial y Rusia, el país más extenso territorialmente a nivel global (IHU, 2018). En cifras, el triángulo RIC representa el 19% del territorio mundial y el 33% del PBI mundial, además de que se trata de tres potencias nucleares, teniendo dos de ellas -Rusia y China- asiento en el Consejo de Seguridad de Naciones Unidas (Purushothaman, 2018).

No obstante, resulta necesario recordar que la idea de un bloque trilateral entre Rusia, India y China, tiene sus primeros indicios en 1998. En aquel año, luego de una visita a la India donde se propuso la cooperación entre las tres naciones, Yevgeni Primakov, por entonces Ministro de Asuntos Exteriores de la Federación de Rusia, estipula lo que se conoció como la "Doctrina Primakov". La misma anunciaba un giro en la política exterior debido a la geopolítica de la época, para mejorar la posición de Rusia a nivel internacional y promover el equilibrio de poder en un panorama multipolar. No menos importante es que se proponía, además, conformar un bloque trilateral estratégico que fuera liderado por Rusia para contrarrestar la supremacía estadounidense. Si bien las respuestas tanto de China como de India, no fueron las esperadas por Rusia, lo cierto es que la idea se institucionalizó unos años después, cuando los ministros de Asuntos Exteriores de los tres países se reunieron por primera vez en el año 2003 y luego en 2005, consolidando la marca diplomática "RIC" como un mecanismo de diálogo entre los tres estados (Singh, 2023).

Si bien los países RIC se caracterizan por estar de acuerdo en establecer un orden mundial de carácter multipolar para contrarrestar la hegemonía estadounidense, es importante remarcar que existen disparidades al interior de sus miembros, en tanto el vínculo entre China e India, por ejemplo, se encuentra sumido en numerosas disputas fronterizas que aún no tienen resolución. Sin embargo, aquí es cuando merece consideración mencionar que Rusia juega un papel de "puente" entre los dos países, ya que posee fuertes y amigables lazos tanto con China como con India (Purushothaman, 2018).

En la actualidad, los encuentros de la tríada sirven de intercambios para identificar temáticas en la que los miembros pueden converger para cooperar. Una de ellas ha sido la cuestión de la seguridad internacional, y en específico, la ciberseguridad, la cual ha ido ganando cada vez más relevancia en las agendas de las grandes potencias.

[2] El superciclo de las materias primas puede ser definido como el aumento sostenido en el tiempo (con una tendencia a largo plazo, es decir, más de cinco años) del precio de las materias primas (alimentos, bebidas, petróleo, metales, productos químicos, combustibles). Esta situación se dio a inicios de la década del 2000 finalizando con la crisis financiera sucedida en 2008 (Taylor, 2022).

Como se mencionó en la introducción de este escrito, en el siglo XXI internet se ha convertido en una herramienta para promover nuevas estructuras y espacios de influencia en lo que se denomina la sociedad de la información. Generalmente, cuando hablamos de internet hacemos referencia a "un instrumento, un medio, y una manifestación tecno-económica de desarrollo humano" (Eriksson & Giacomello, 2009, p. 211).

En este ámbito, diferentes grupos de interés, así como también los Estados, llevan adelante acciones para conseguir sus intereses en la esfera del ciberespacio, zona no regulada internacionalmente. En efecto, la protección de internet resulta invaluable (Aspis, 2014), por lo cual los gobiernos de las grandes potencias se han encargado de revisar sus regulaciones, así como los mecanismos que puedan asegurar a sus usuarios el uso seguro de los sistemas de información. En otras palabras, las grandes potencias pueden, llegado el caso de una situación crítica, administrar sus propias estructuras de las comunicaciones nacionales para restringir los accesos u obstaculizar el ingreso a internet (Aguirre Azócar y Morandé Lavín, 2017).

Como se ha mencionado, la ciberseguridad ha cobrado importancia en los últimos años, cuestión por la cual los gobiernos se han mostrado preocupados por desarrollar mayores y mejores controles del ciberespacio. En este punto, es de vital importancia marcar la diferencia, de manera clara y sencilla, entre los conceptos de **ciberespacio** y ciberseguridad. Cuando hacemos referencia al primero de ellos, hablamos de un entorno virtual, común y sin fronteras, donde se intercambia la información (Choucri, 2012); en nuestras palabras, podemos decir que se trata del ámbito digital donde se desarrollan las redes y actividades en línea, además de los sistemas informáticos. Por su parte, en rasgos generales, el término de **ciberseguridad** se asocia a la seguridad de la tecnología de la información, incluyendo numerosas técnicas y métodos para la protección de los sistemas, los dispositivos y las redes (Rosas Bello *et al.*, 2020). Así la ciberseguridad hace referencia a un conjunto de prácticas preventivas para garantizar la seguridad y protección de esa información que es intercambiada ante posibles accesos no autorizados, ataques cibernéticos, robos de datos confidenciales o daños a los sistemas (Zdzikot, 2021; De Groot, 2023).

Bajo este contexto, el ciberespacio está en miras de los gobiernos para ser el próximo espacio a regular de manera internacional. Mientras tanto, los estados ya han aplicado diferentes estrategias con el objetivo de establecer leyes que regulen el control del flujo de la información en red y la salvaguardia de sus intereses nacionales (Schreiber, 2019). Por estos motivos, a continuación, analizaremos las concepciones y tratamientos desarrollados por cada país del triángulo RIC respecto del ciberespacio y la ciberseguridad.

2. Concepción y estrategia de ciberseguridad de los países miembros de RIC

A la hora de hablar de las concepciones que poseen cada uno de los países miembros del triángulo RIC y cuáles son las estrategias que sus gobiernos implementan en dicha materia, podemos identificar diversos enfoques nacionales que ameritan un abordaje por separado.

Federación Rusa

Desde la mirada del Kremlin, la cuestión del internet es una parte importante y delicada de la estrategia de política nacional, así como también de la política exterior, en tanto las actividades cibernéticas se convierten para este país, en un espacio de "*information confrontation*"[3] entre los diversos estados. De esta forma, la Federación Rusa (en adelante, Rusia) despliega una postura ofensiva frente a la percepción de amenaza en su exterior cercano, lo cual se ve reflejado en la Doctrina de Seguridad de la Información[4] del año 2016 que estipula:

> Los servicios de inteligencia de ciertos Estados utilizan cada vez más la información y las herramientas psicológicas con miras a desestabilizar la situación política y social interna en diversas regiones del mundo, socavando la soberanía y violando la integridad territorial de otros Estados. Las organizaciones religiosas, étnicas, de derechos humanos y otras organizaciones, así como grupos separados de personas, participan en estas actividades y las tecnologías de la información se utilizan ampliamente con este fin (Security Council of the Russian Federation, 2016).

De esta manera, ya desde el año 2000, Rusia comenzó a priorizar los medios no militares para contrarrestar la amenaza de sus rivales. La defensa del ciberespacio se ha convertido en una preocupación primordial para el Kremlin en el corriente siglo. Por lo tanto, el control del mismo conforma uno de los elementos estratégicos del país a la hora de reafirmar su poder (Duparc, 2017).

Sin embargo, antes de continuar, debemos aclarar que como vimos con el nombre de la Doctrina, en el caso ruso no se utiliza el concepto de "*cibersecurity*", sino más bien el de "*information security*", debido a que este último término incluye no solamente la protección de las redes digitales de internet, sino también la integridad cognitiva de la sociedad civil. De hecho, en la Doctrina mencionada, el concepto es definido de la siguiente manera:

> El estado de protección del individuo, la sociedad y el Estado contra las amenazas de información internas y externas, que permite garantizar los derechos humanos y civiles constitucionales y las libertades, la calidad y el nivel de vida dignos de los ciudadanos, la soberanía, la integridad territorial y el desarrollo socioeconómico sostenible de la Federación de Rusia, así como la defensa y la seguridad del Estado (Security Council of the Russian Federation, 2016)[5].

En consecuencia, los esfuerzos de Rusia en este ámbito, tienen por objetivo liderar la iniciativa en cuestiones de seguridad y gobernanza cibernética. Para ello, Moscú entiende que se permite cualquier tipo de medio para alcanzar la superioridad, por lo cual desde el gobierno se han estado utilizando las operaciones cibernéticas como complemento a los medios militares y no militares, para la consecución de los objetivos estratégicos. Explícitamente, las armas de información o

[3] La traducción del término "information confrontation" se hace muchas veces de manera incorrecta por el término "guerra de información". Los términos en español que más se acercan a la definición en español son "confrontación" o "lucha".

[4] Según el sitio oficial del Consejo de Seguridad de la Federación Rusa, la Doctrina mencionada se constituye por un sistema de principios de carácter oficial sobre cómo proteger la seguridad nacional del país en el ámbito de la información (Security Council of the Russian Federation, 2016).

[5] Traducción al español del idioma original de la fuente realizada por las autoras.

"*information weapons*" -como se suele utilizar en Rusia, pero no en Occidente- incluyen la difusión de desinformación, la guerra electrónica, la degradación del soporte de navegación, la presión psicológica y la destrucción de las capacidades informáticas del adversario (Russian Federation, 2011).

Ahora bien, según el Ministerio de Defensa de Rusia, esta "*information confrontation*" de la que hablamos, es comprendida como el choque de intereses e ideas nacionales, donde se busca la superioridad (independientemente de si se está en un conflicto o no) apuntando a la infraestructura de información del adversario mientras se protegen los objetos propios de influencia similar (Veprintsev *et al*., 2015). Para una mayor comprensión, esta confrontación se da en la mente y en la percepción de las personas, jugando el factor psicológico un papel extremadamente importante. En otras palabras, el actor en cuestión intenta entrometerse en los recursos de información disponibles, así como también en las mentes de sus adversarios, ya sea de la población o del personal militar. De esta forma, según la perspectiva del Kremlin, en esta confrontación se da una lucha geopolítica constante y de suma cero entre las grandes potencias y sus respectivos sistemas políticos, económicos y sociales (Kukkola et al., 2017).

Bajo este marco, debemos preguntarnos cuál es el ámbito de aplicación de la Doctrina anteriormente mencionada. En cuanto a ello, Rusia vuelve a marcar diferencia con la noción occidental, en tanto no utiliza el término de "*cyberspace*", sino más bien el de "*information space*" o "*information sphere*", para incorporar en este concepto una:

> (...) combinación de información, objetos de informatización, sistemas de información y sitios web dentro de la red de información y telecomunicaciones de internet, redes de comunicación, tecnologías de la información, entidades involucradas en la generación y el procesamiento de la información, el desarrollo y uso de las tecnologías mencionadas y la garantía de la seguridad de la información, así como un conjunto de mecanismos que regulan las relaciones públicas en la materia (Security Council of the Russian Federation, 2016)[6].

Aquí vemos entonces cómo el Kremlin hace una lectura geopolítica a partir de la defensa del concepto tradicional de soberanía (en este caso, soberanía digital) y el principio de no intervención en el centro de su política hacia el internet global. En otras palabras, la esfera de información es concebida como un territorio con fronteras virtuales correspondientes a las fronteras físicas del Estado, sobre el cual Rusia busca extender la aplicación de sus leyes nacionales (Kukkola & Ristolainen, 2018).

En relación a ello, Moscú estableció la Ley de Soberanía de internet o "internet soberano de Rusia" en el año 2019, la cual se focaliza en la protección de sus ciudadanos frente a los ataques cibernéticos. Con esta finalidad, la ley permite que el gobierno pueda desconectar y aislar el segmento ruso de internet, denominado "RuNet", del internet a nivel global. Para ello, el objetivo principal es tener para el año 2024, solamente el 10% del tráfico de internet ruso enrutado a través de servidores extranjeros. En breve, el país intenta cada vez más, asegurar y garantizar la independencia de su propia red global de internet en vistas de poder fortalecer la

[6] Traducción al español del idioma original de la fuente realizada por la autoras.

seguridad de su información (Zanfir-Fortuna & Iminova, 2021) y lograr una independencia de los medios occidentales.

A su vez, Rusia decidió modificar en el año 2021, la Ley de Protección de Datos, así como también la Ley de Información. Las enmiendas a la primera ley establecieron nuevos requisitos para el intercambio de los datos personales, así como nuevas funciones de monitoreo y supervisión del Regulador Federal de Medios e Información. Por su parte, las enmiendas a la Ley de Información apuntaron a restringir el acceso de manera inmediata a aquellos usuarios que compartieran información sensible, como secretos de estado, terrorismo, pornografía, promoción de la violencia o disturbios (Belli, 2021).

Bajo este análisis exhaustivo, podemos considerar que existe un objetivo concreto en materia de ciberseguridad, el cual consiste en proteger la información en una red nacional avalada por las propias leyes rusas para poder lograr así un internet nacional soberano e independiente de Occidente. Sin embargo, no existe en la Federación de Rusia una regulación unificada sobre la materia de ciberseguridad, por lo cual, dependiendo de cada caso particular, los principios que pueden ser aplicables.

A modo de cierre, resulta importante mencionar las distintas autoridades reguladoras que existen en el país. Entre ellas se encuentran, además del gobierno de la Federación de Rusia quien está a cargo de desarrollar la política estatal, el Ministerio de Desarrollo Digital, Comunicaciones y Medios de Comunicaciones, principal órgano ejecutivo en el ámbito de las TICs y el procesamiento de datos. Asimismo, Rusia cuenta con el Roskomnadzor - Servicio Federal de Supervisión de Comunicaciones, Tecnologías de la Información y Medios de Comunicación - el cual lleva adelante el control sobre los servicios de comunicación a través de inspecciones, prescripciones y trámites administrativos (Gulyaeva et al., 2022).

República Popular China

La República Popular China (en adelante, China) tiene en claro el hecho de que la tecnología ha avanzado de manera muy rápida, por lo cual el gobierno se ha preocupado constantemente por mantenerse en el mismo ritmo, aumentando la capacidad del propio Estado para controlarla. En este sentido, en el caso del gigante asiático, la cuestión del ciberespacio y los datos, se vincula más al concepto de soberanía gubernamental, motivo por el cual se están estableciendo en el país cada vez más políticas y normas para la protección de los datos. Ya desde la Constitución nacional, China pone énfasis en los derechos de privacidad y los principios de seguridad, basándose en tres bases legales, como son la Ley de Ciberseguridad (CSL), la Ley de Seguridad de Datos (DSL) y la Ley de Protección de Información Personal (PIPL) (Wang et al., 2022).

Antes de analizar cada una de las normas mencionadas, debemos recordar que, para el gobierno chino, la ciberseguridad hace referencia no sólo a conceptos como integridad, confidencialidad y disponibilidad de la información, sino también a la relevancia que adquiere el carácter sensible de la misma, por lo cual el acceso pasa a ser restringido siguiendo lo establecido por el marco jurídico nacional. En este sentido, China considera que “la confidencialidad de esta información estratégica fortalece su ejercicio gubernamental y, a su vez, permite el desarrollo y el bienestar general de la sociedad”. Desde esta perspectiva entonces, Patiño Orozco resalta que la ciberseguridad es considerada por la República Popular como un instrumento para

reducir los potenciales riesgos que puedan afectar la legitimidad y el margen de acción política; de ahí que la visión de este país haga más foco en aspectos socio-políticos y no tanto en aspectos técnicos (Patiño Orozco, 2021, p. 111).

Bajo este marco, ahora podemos mencionar que la CSL, adoptada en noviembre de 2016 y en vigor desde junio de 2017, es el pilar jurídico fundamental y cúspide del resto de las regulaciones en vistas de constituir un ciberespacio chino soberano, en tanto es la que establece el marco general de seguridad. Su marco de aplicación incluye a todos los operadores de redes, es decir, propietarios, administradores y proveedores de un sistema formado por computadoras y equipos que recopilan, almacenan, transmiten, intercambian o procesan información. En otras palabras, la ley resulta aplicable a la mayoría de las empresas en China que poseen redes de datos. Entre los artículos destacados, vale mencionar el número 37, en el cual se estipula que la información comercial y los datos de ciudadanos chinos se mantengan en servidores nacionales y no se transfieran al extranjero sin previa autorización; así como también recalca la prohibición de exportar datos económicos, tecnológicos o científicos que puedan peligrar la seguridad nacional o el interés público del país (Wagner, 2017).

Las otras dos leyes mencionadas, la DLS y la PIPL, entraron en vigor en el año 2021 y tienen en común que ambas reclaman poder extraterritorial para proteger los datos y la información personal procesados por la infraestructura protegida por la CSL. Sumado a esto, existen penalidades por el procesamiento de datos que pueda resultar perjudicial para la seguridad nacional, el interés público o los derechos e intereses de un ciudadano chino (Wang et al., 2022). De esta manera, China consolidó la idea que había plasmado en el Libro Blanco del año 2010: “dentro del territorio chino, internet está bajo la soberanía de China” (Wagner, 2017).

La DSL se basa en la protección de los datos procesados, para lo cual establece una regulación para el almacenamiento y la transferencia de los mismos. Para ello, la ley divide los datos en una clasificación: los datos básicos, entendidos como aquellos relacionados con la seguridad nacional, el bienestar de los ciudadanos chinos y los intereses públicos; y los datos importantes, los cuales no fueron definidos en su alcance (Junck et al., 2021).

Por otro lado, la PIPL regula el procesamiento de la información personal, la cual es definida como “cualquier información relacionada con personas físicas identificadas o identificables almacenada en formato electrónico o de cualquier otro formato”[7] (Junck et al., 2021, p. 2). Esta ley en particular, establece que la información personal sólo puede ser exportada del país luego de cumplir ciertos requisitos, además de la obtención de la aprobación regulatoria. Entre los pasos a seguir, se encuentran: aprobar una evaluación de seguridad de la Administración del Ciberespacio de China (CAC), obtener una certificación de protección de información personal de una institución profesional designada por la CAC o celebrar un acuerdo de transferencia de datos de formato estándar con el destinatario extranjero de dichos datos (Fang & Liang, 2022).

Para concluir, debemos considerar un último dato importante: la entrada en vigor el 1 de enero de 2021 del Código Civil. Allí se estableció, en el Capítulo VII de la Parte IV sobre Derechos de la persona, el derecho a la privacidad y la protección de la información personal. En este sentido, para Dora Luo y Yanchen Wang, especialistas en derecho corporativo, de privacidad y de ciberseguridad, China ha comenzado una nueva

[7] Traducción al español del idioma original de la fuente realizada por las autoras.

era en la protección de la información y de los datos. Las autoras sostienen que se espera que, en un futuro cercano, el país continúe estableciendo normas, así como avanzando y evolucionando las reglas ya establecidas en el campo de la legislación para la protección de su información (Luo & Wang, 2023).

República de India

El caso de la República de India (India, en adelante) resulta particular, porque, a pesar de su gran posición en el sistema internacional y de su relevante economía en la industria 4.0 (Fernández Aparicio, 2022), es catalogada como uno de los países menos ciberseguros a nivel global, ocupando el puesto número 15 donde el número uno es el menos seguro (Rampal, 2019). En este sentido, los diferentes gobiernos que han estado en el poder, han intentado progresivamente otorgar mayor prioridad a la cuestión de la ciberseguridad, en tanto se corresponde como una necesidad ineludible para la seguridad nacional (Fernández Aparicio, 2022).

Si bien podemos encontrar leyes y regulaciones desde 1885 con la Ley de Telégrafos o más cercanas en el tiempo con la *Information Technology Act* del año 2000, la política india vinculada a ciberseguridad data del año 2013, cuando el Ministerio de Comunicación y Tecnología de la Información publicó la Política de Ciberseguridad Nacional India (PCNSI) en vistas de lograr un ciberespacio más seguro y resiliente para las operaciones en la red por parte de los ciudadanos, las empresas y el gobierno, así como también de disminuir los ataques cibernéticos. En ella se establecieron 14 objetivos ambiciosos que incluían la protección de la infraestructura crítica, el procesamiento de delitos cibernéticos y la capacitación y creación de una fuerza laboral de 500 mil profesionales en ciberseguridad (Tomar, 2013).

Entre los años 2014 y 2015, el Departamento de Tecnología de Información de India, destinó 1.160 millones de rupias indias (15.7 millones de euros) para la seguridad cibernética. Asimismo, el país se propuso crear un Centro Nacional de Coordinación Cibernética (CNCC) con un presupuesto de aproximadamente 10.000 millones de rupias indias, lo que equivale a más de 136 millones de euros. El mismo entró en funcionamiento a principios de agosto de 2017 con la función principal de monitorear el flujo de datos en línea del país para identificar posibles riesgos y amenazas para la seguridad informática (PTI News Agency, 2017). Por otro lado, si bien India posee un gran recurso humano experto en matemáticas y ciencias de la computación, también se ha preocupado por conseguir apoyo en materia de formación para mejorar su seguridad cibernética, para lo cual ha enviado delegaciones de funcionarios y empresarios a Londres, La Haya e Israel (Hinarejos Rojo y de la Peña Muñoz, 2017).

Luego de la pandemia por el COVID-19 y debido al inevitable avance de la tecnología, en conjunto con mayores reclamos por parte de diversos sectores para actualizar la política nacional, India se vio obligada a comenzar a revisar sus estrategias para prevenir las amenazas en el ciberespacio. Aquí resulta interesante mencionar que estamos hablando del país más poblado del mundo, compuesto por 1.400 millones de habitantes, de los cuales 658 millones son usuarios de internet y de ese total, 467 lo son de las redes sociales (Fernández Aparicio, 2022).

Cabe remarcar que, aunque con una cierta indefinición entre las atribuciones, India cuenta con diversos organismos encargados de velar por la seguridad del ciberespacio nacional. Entre ellos, podemos mencionar el *National Technical*

Research Organisation (NRTO), como cabeza de las instituciones de ciberseguridad en tanto es la encargada de recopilar los datos de inteligencia y transmitirlos a la Administración india. Dentro de la NRTO, se encuentran dos agencias: por un lado, la *National Critical Information Infrastructure Protection Centre* (NCIIPC), que aboga por la protección de infraestructuras críticas ante ataques cibernéticos; y, por otro lado, el *National Institute of Cryptology Research and Development* (NICRD), organismo a cargo del cifrado seguro para las aplicaciones cibernéticas de las infraestructuras críticas. A su vez, India cuenta con el *National Cyber Coordination Centre* (NCCC), el cual tiene la función de concientizar a la sociedad civil sobre la relevancia de la ciberseguridad; el *Indian Computer Emergency Response Team (CERT-In),* quien despliega instrucciones para evitar sitios webs maliciosos y el *Research and Analysis Wing* (RAW), centrada en la relación entre política exterior y seguridad nacional, sobre todo respecto a Pakistán y China (Fernández Aparicio, 2022).

Sin embargo, luego de todo lo descrito, India continúa aún sin actualizaciones en el campo de su estrategia nacional para la ciberseguridad, que proviene del año 2013. Incluso, a pesar de la existencia de numerosos organismos para el trabajo en esta materia, no hay una institución central y unitaria que pueda coordinar todos los esfuerzos.

3. Cooperación de la tríada RIC en materia de ciberseguridad

Si bien el presente artículo tiene su foco puesto en la tríada RIC, resulta importante mencionar que en el año 2021 todos los países miembros de BRICS declararon su compromiso para abogar por una mayor cooperación en materia de ciberseguridad, a tal punto de establecer marcos regulatorios entre las partes (BRICS, 2021). Como antecedente a este hecho, debemos remontarnos al año 2013, cuando los BRICS afirmaron su deseo de incrementar los esfuerzos para un ciberespacio pacífico, seguro y abierto, a través de la implementación de normas y prácticas universalmente aceptadas (BRICS, 2013).

En este contexto, en el año 2016, los Ministros de Asuntos Exteriores de los tres países se reunieron en Moscú el 18 de abril, donde coincidieron en cooperar trilateralmente para la construcción de una sólida arquitectura de seguridad en la región del Asia Pacífico (Singh, 2023). Desde entonces la cooperación en esta área entre las partes se ha incrementado, por lo que aquí haremos referencia a las relaciones RIC en el aspecto de la ciberseguridad. No obstante, es imprescindible remarcar que Rusia, India y China también han llevado adelante iniciativas vinculadas al tema de estudio dentro de Naciones Unidas, así como dentro la Organización de Cooperación de Shanghái (SCO, por sus siglas en inglés). En conjunto, los tres países "conciben que la mejor manera de afrontar la vasta cantidad de problemas de ciberseguridad es a través de la creación de jurisdicciones, normas y reglamentaciones soberanas sobre el flujo de información y contenido en el ciberespacio" (Patiño Orozco, 2021, p. 114).

En este sentido, el triángulo RIC ha estado prestando cada vez más atención a la problemática de la ciberseguridad, aunque debemos decir que, si bien la cooperación se da en el ámbito de las estrategias exteriores, resulta ambicioso pensar en que se logre un sólido bloque político-militar al que podríamos llamar "alianza".

En este marco, es evidente que tanto Rusia como China, han promovido a lo largo de los años la idea de "cibersoberanía" o, en otras palabras, lo que se entiende como el derecho del propio Estado a regular internet en vistas de proteger su interés nacional (Jinda, 2022). Sin embargo, a pesar de la afinidad existente en esta materia, no se ha logrado un gran progreso en la cooperación en materia de ciberseguridad entre los

países. Esto se ve reflejado en que a pesar de los entendimientos que existen entre ambos, se ha demostrado un gran retraso en el cumplimiento de los mismos.

En la misma línea, la idea de un nulo avance en la cooperación entre las partes, también fue se vio reflejada en las palabras de Shen Dingli, el vicedecano del Instituto de Estudios Internacionales de la Universidad de Fudan, una voz destacada en los debates sobre política exterior china. Dingli expresó en junio de 2016 que "China es un país realista" que no forma alianzas a largo plazo y que la cooperación con Rusia es simplemente lo que resulta ventajoso por el momento para "contrarrestar a Estados Unidos". Asimismo, agregó que "ninguna de ellas son estrategias a largo plazo, sino sólo cooperación táctica" (Davidson, 2016).

Por su parte, Rusia ha afianzado su vínculo en el ámbito cibernético con la República de India, aunque eso no ha significado una cooperación más sólida. Sin embargo, aquí no debemos dejar de mencionar el primer acuerdo de seguridad cibernética entre estos países en el año 2016, el cual estableció un "Diálogo de Alto Nivel sobre Cuestiones Cibernéticas". En el mismo, se estipulan las pautas para llevar adelante la cooperación conjunta en la protección de las infraestructuras críticas y la lucha contra el delito cibernético (Jinda, 2022).

Luego, en el año 2021, ambos países llegaron a la decisión de dinamizar la colaboración entre organizaciones gubernamentales y el sector privado para crear de manera conjunta, plataformas, servicios y productos de *software* frente a las amenazas a la ciberseguridad (Jinda, 2022).

A raíz de lo analizado en este apartado, podemos considerar que es evidente que los países de la triada RIC poseen cierto interés en alcanzar un mayor grado de cooperación en el ámbito de la ciberseguridad. Sin embargo, como consecuencia de las divergencias que existen entre ellos debido a los respectivos intereses nacionales, los intentos de mayor colaboración entre las partes no han sido suficientes para alcanzar un mayor estadio en la cuestión que aquí nos compete.

Reflexiones finales

Como hemos visto a lo largo de este artículo, el ciberespacio ha ido adquiriendo mayor relevancia en las agendas de los Estados, sobre todo con el rápido avance de las TICs y luego de la pandemia de COVID-19. En este sentido, los países han desarrollado un tratamiento diferenciado intentando establecer y aplicar regulaciones para salvaguardar los intereses nacionales.

De esta manera, Rusia entiende a la ciberseguridad como un asunto delicado perteneciente a la política doméstica, pero también externa. A partir de una percepción de "confrontación de la información" en el ciberespacio, el Kremlin ha adoptado una postura ofensiva donde se incluyen también aspectos de la mente de las personas. En tanto, desde una lectura geopolítica que conjuga la soberanía digital y el principio de no intervención, Rusia se encuentra en el camino de querer asegurar y garantizar la independencia de su propia red frente a los medios occidentales.

En efecto, encontramos aquí una similitud con la República Popular China, quien vincula el ciberespacio y la esfera de los datos también con la idea de soberanía gubernamental. Se considera que la ciberseguridad hace referencia al intercambio de información sensible y que, por ende, debe ser restringido y protegido. En otras palabras, las posturas tanto china como rusa, hacen referencia al objetivo de

pasar de un internet basado en una red informática mundial a una red informática nacional que opere bajo un sólido sistema de protección de la información. Ambas estrategias buscan desarrollar sus propias herramientas digitales, independientes de la red global occidental, donde poder conservar y proteger los datos nacionales.

El caso de India, como hemos dilucidado en los apartados anteriores, es particular, ya que se trata de uno de los países menos ciberseguros a nivel global. A pesar de que con el tiempo la temática ha ido adquiriendo un grado mayor de prioridad en la agenda del gobierno indio, no hemos encontrado en la bibliografía rastros de actualizaciones de las estrategias o regulaciones para prevenir las amenazas del país.

Hasta aquí entonces, hemos dado respuesta a nuestro interrogante acerca de cómo han abordado los países RIC los desafíos de la ciberseguridad durante el siglo XXI. Pero si nos preguntamos sobre la existencia de programas de cooperación, agendas comunes o estrategias conjuntas, debemos decir que a pesar de haber compromisos entre los países RIC, se trata de meros discursos que no han conseguido el total cumplimiento de cada una de las partes.

En efecto, retomando la Doctrina Primakov de un bloque trilateral estratégico, liderado por Rusia y que sirviera de contrapeso a Estados Unidos, podemos decir que aún 25 años después, los encuentros periódicos entre Rusia, India y China no han conducido a aquel deseo. El diálogo y la discusión para la cooperación conjunta no se han transformado todavía en una plataforma estratégica trilateral. Las reuniones entre los tres países se limitan a un grupo de discusión y se le atribuye ser el precursor de plataformas no occidentales exitosas como los BRICS y la SCO, lo cual indica, además, que India y China, a pesar de sus disputas fronterizas, se encuentran cooperando a mayor escala. Si bien Rusia disfruta de relaciones cordiales tanto con China como con la India, la transformación del RIC en una plataforma para la cooperación cibernética requeriría mayores esfuerzos de cooperación entre los tres países (Singh, 2023).

En este punto, es pertinente remarcar que existen diversos factores que han actuado como obstáculos para que el RIC ganara impulso. En primer lugar, el hecho de que Rusia, India y China tengan sistemas políticos completamente diferentes, es el mayor impedimento para un alcanzar el desarrollo de sus vínculos trilaterales. En segundo lugar, la divergencia de opiniones entre el público y las elites dificulta cualquier cooperación entre el triángulo RIC. En este sentido, Rusia considera al RIC como una herramienta geopolítica para contrarrestar a Occidente y no como una gran estrategia. India por su parte mantiene una actitud cautelosa hacia el RIC, debido a su principio utilitario y su sensibilidad ante la percepción estadounidense de que la India tiene una relación más estrecha con Rusia y China. Finalmente, las preocupaciones y disputas de seguridad son otros obstáculos para cualquier cooperación en el RIC. Por lo tanto, será necesario que el RIC resuelva problemas a nivel operativo, el déficit de confianza y la débil cooperación en ámbitos no políticos (Singh, 2023). En otras palabras, será imprescindible que Rusia, India y China vayan detrás de una visión y una meta comunes para consolidar el vínculo triangular en una asociación estratégica de mayor peso internacional.

Referencias bibliográficas

Aguirre Azócar, D., y Morandé Lavín, J. (2017). El desarrollo global del ciberespacio: nuevos desafíos para los Estados y la sociedad civil. InterNaciones. https://internaciones.cucsh.udg.mx/index.php/inter/article/view/6894/6203

Aspis, A. (2014). La gobernanza de Internet y la nueva agenda mundial de los recursos tecnológicos. XLIII Jornadas Argentinas de Informática e Investigación Operativa. Sociedad Argentina de Informática e Investigación Operativa (SADIO). http://sedici.unlp.edu.ar/handle/10915/42070

Belli, L. (2021). Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *The African Journal of Information and Communication (AJIC),* 28, 1-14. https://doi.org/10.23962/10539/32208

BRICS. (2013). eThekwini Declaration and Action Plan. https://www.mea.gov.in/bilateral-documents.htm?dtl/21482

BRICS. (2021). BRICS India 2021 - XIII BRICS Summit - New Delhi Declaration. brics2021.gov.in/brics/public/uploads/docpdf/getdocu-51.pdf

Chislova, O., & Sokolova, M. (2021). Cybersecurity in Russia. *International Cybersecurity Law Review,* 2(2), 245-251. https://doi.org/10.1365/s43439-021-00032-9

Chen, J., Scott, G., & Eichler, R. (2023). BRICS: Acronym for Brazil, Russia, India, China, and South Africa. *Investopedia*. https://www.investopedia.com/terms/b/brics.asp

Choucri, N. (2012). Cyberpolitics in International Relations. Cambridge: The MIT Press. https://www.jstor.org/stable/j.ctt5hhkrs

Davidson, L. (2016). Despite Cyber Agreements, Russia and China Are Not as Close as You Think. *Council On Foreign Relations*. https://www.cfr.org/blog/despite-cyber-agreements-russia-and-china-are-not-close-you-think

De Groot, J. (2023). What is cyber security? Definition, best practices & examples. *Digital Guardian.* https://www.digitalguardian.com/blog/what-cyber-security

Duparc (2017). Cómo Rusia reclutó y formó a «batallones» de hackers. *Nueva sociedad,* 269. https://nuso.org/articulo/como-rusia-recluto-y-formo-batallones-de-hackers/

Eriksson, J., & Giacomello, G. (2009). Who controls the internet? Beyond the obstinacy or obsolescence of the State. *International Studies Review*, 11(1), 205-230. https://academic.oup.com/isr/article-abstract/11/1/205/1846467

Fang, S., & Liang, H. (2022). Chinas Emerging data protection laws bring challenges for conducting investigations in China. DLA Piper. https://www.dlapiper.com/en/insights/publications/2022/07/chinas-emerging-data-protection-laws-bring-challenges-for-conducting-investigations-in-china

Fernández Aparicio, J. (2022). Ciberseguridad en la India: bilateralidad y transformación. *Instituto Español de Estudios Estratégicos (IEEE),* (26), 454-468. https://www.ieee.es/en/publicaciones-new/documentos-de-analisis/2022/DIEEEA37_2022_JAVFER_India.html

Gulyaeva, N., Gurieva, J., & Gorbushina, A. (2022). Russia: Cybersecurity. DataGuidance.https://www.dataguidance.com/opinion/russia-cybersecurity

Hinarejos Rojo, A., y de la Peña Muñoz, J. (2017). I+D+i y ciberseguridad: análisis de una relación de interdependencia. *Cuadernos de Estrategia*, (185), 247-290. https://dialnet.unirioja.es/descarga/articulo/6115626.pdf

IHU. (2018). Fraco B-RIC-S, forte RIC: o triângulo estratégico que desafia os EUA e o Ocidente. Instituto Humanitas Unisinos (IHU). https://www.ihu.unisinos.br/categorias/188-noticias-2018/579816-fraco-b-ric-s-forte-ric-o-triangulo-estrategico-que-desafia-os-eua-e-o-ocidente

Jinda, D. (2022). Can India & Russia resuscitate cyber relationship? Info BRICS. https://infobrics.org/post/36144/

Junck, R. D., Klein, Kumaki, Kumayama, K. D., Kwok, S., Levi, S. D., Talbot, J. S., Vermynck, E. C., & Zhang, S. (2021). China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies. Skadden. https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws

Kukkola, J., &Ristolainen, M. (2018). Projected territoriality: A case study of the infrastructure of Russian 'digital borders'. *Journal of Information Warfare*, 17(2), 83-100. https://www.researchgate.net/publication/326292919_Projected_territoriality_A_case_study_of_the_infrastructure_of_Russian_'digital_borders'

Kukkola, J., Ristolainen, M., & Nikkarila, J. P. (2017). Game Changer: Structural transformation of cyberspace. *Finnish Defence Research Agency Publications.* https://maavoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398/PVTUTKL+julkaisuja+10.pdf.pdf

Luo, D., & Wang, Y. (2023). China - Data Protection Overview. DataGuidance. https://www.dataguidance.com/notes/china-data-protection-overview

O'Neill, J. (2001, 30 noviembre). Building Better Global Economic BRICs. Goldman Sachs Global Economic Paper No. 66. https://www.goldmansachs.com/intelligence/archive/archive-pdfs/build-better-brics.pdf

Patiño Orozco, Germán Alejandro (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos, *OASIS,* 34, 107-126. https://www.redalyc.org/journal/531/53169476007/html/#:~:text=Para%20el%20gobierno%20chino%2C%20la,grupos%20bajo%20un%20marco%20jur%C3%ADdico.

PTI News Agency. (2017). Cyber Coordination Centre made operational: IT Ministry. *The Indian Express*. https://indianexpress.com/article/india/cyber-coordination-centre-made-operational-it-mininstry-4789272/

Purushothaman, U. (2018). Why RIC is as important to India as JAI and BRICS. *Observer Research Foundation (ORF)*. https://www.orfonline.org/expert-speak/why-ric-is-as-important-to-india-as-jai-and-brics-46213/

Rampal, N. (2019). India's cybersecurity a joke for hackers, ranks among worst in the world. India Today. https://www.indiatoday.in/india/story/india-cybersecurity-privacy-data-breach-crypto-hackers-aadhaar-1450572-2019-02-07

Rosas, W. A., Medina, F. A., & Mesa, J. A. (2020). Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas. *Revista Espacios*, 41(07). http://ww.w.revistaespacios.com/a20v41n07/20410727.html

Russian Federation. (2011). Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. https://nsarchive.gwu.edu/document/17098-russian-government-conceptual-views-regarding

Schreiber, C. (2019). El futuro de China y Rusia como aliados en el ciberespacio. Grupo de Estudios en Seguridad Internacional (GESI), 2(1). https://www.seguridadinternacional.es/?q=es/content/el-futuro-de-china-y-rusia-como-aliados-en-el-ciberespacio

Security Council of the Russian Federation. (2016). Doctrine of Information Security of the Russian Federation. The Ministry of Foreign Affairs of the Russian Federation. http://www.scrf.gov.ru/security/information/DIB_engl/

Singh, R. (2023). Russia, India and China Alliance – towards balancing the world Order. Defence Research and Studies. https://dras.in/russia-india-and-china-alliance-towards-balancing-the-world-order/?

Taylor, H. (2022). What is a commodity supercycle and are we in one right now? *Capital Com SV Investments Limited*. https://capital.com/commodity-supercycle-explained

Tomar, S. (2013). National Cyber Security Policy 2013: An Assessment. Manohar Parrikar Institute for Defence Studies and Analyses. https://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813

Veprintsev, V., Manoylo, A., & Petrenko, A. (2015). Russian Federation. Information confrontation, Dictionary of Terms. Russian Ministry of Defence.

Wagner, J. (2017). China's cybersecurity law: What you need to know. *The Diplomat*. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

Wang, V; Xinyao Z. & Wang E. (2022). Una comparación de las regulaciones de ciberseguridad: China. Revista de derecho empresarial de Asia. https://law.asia/china-cybersecurity-regulations-2022/

Zanfir-Fortuna, G., & Iminova, R. (2021). Russia: New law requires express consent for making personal data available to the public and for any subsequent dissemination. Future of Privacy Forum. https://fpf.org/blog/russia-new-law-requires-express-consent-for-making-personal-data-available-to-the-public-and-for-any-subsequent-dissemination/

Zdzikot, T. (2021). Cyberspace and cybersecurity. En *Cybersecurity in Poland*, 9-21 https://doi.org/10.1007/978-3-030-78551-2_2

Cómo citar:

CAPELLINO. M., VIRGILI, C. (2024). Los desafíos en materia de ciberseguridad en el siglo XXI en las relaciones sino-rusa e indo-rusa. *Revista Integración y Cooperación Internacional,* 39 (Jul-Dic), 20-35