REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL

unicuritiba

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

RELACIONES INTERNACIONALES Y GEOPOLÍTICA: CONFLICTO Y PODER EN EL CIBERESPACIO

INTERNATIONAL RELATIONS AND GEOPOLITICS: CONFLICT AND POWER IN CYBERSPACE

GABRIELA MATA-SÁNCHEZ
Research Department Coordinator. Coordinator of the PhD program in International Relations, Business and Diplomacy. Universidad Autónoma de Nuevo León. México. ORCID iD http://orcid.org/0000-0003-0590-0174

RESUMEN
Armado o no, el conflicto es una constante en las relaciones internacionales y ha sido objeto de estudio de diversas disciplinas. Si acaso, la variable es el escenario en el que sucede. El presente artículo realiza un análisis teórico y documental sobre el ciberespacio como nuevo escenario de conflicto en la arena internacional y las implicaciones desde la Geopolítica, pues esta nueva dimensión es de importancia vital para el actuar de los Estados, la definición de sus intereses nacionales, el control de los flujos de información, la delimitación de sus nuevas fronteras espaciales y la distribución del poder en las relaciones internacionales. El ciberespacio replica comportamientos de los Estados en el ámbito tradicional, pero con características como una indefinición de las fronteras, mayor participación del sector privado, mayor involucramiento de la sociedad civil y, en general, mayor complejidad para garantizar la seguridad y la supervivencia.

Palabras clave: geopolítica; ciberespacio; conflicto.

ABSTRACT
Armed or not, conflict is a constant issue in international relations and has been the subject of study in various disciplines. If anything, the variable is the setting in which it happens. This article carries out a theoretical and documentary analysis of cyberspace as a new scenario of conflict in the international arena and the implications from Geopolitics, since this new dimension is of vital importance for the actions of States, the definition of their national interests, the control of flows of information, the delimitation of its new spatial borders and the distribution of power in international relations. Cyberspace replicates the behavior of States in the traditional sphere, but with characteristics such as the lack of definition of borders, greater participation of the private sector, greater involvement of civil society and, in general, greater complexity to guarantee security and survival.

Keywords: geopolitics; cyberspace; conflicto.

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

1 INTRODUCCIÓN

A lo largo de lo que los internacionalistas identificamos como Historia de las Relaciones Internacionales, el conflicto (armado o no) ha sido, si no es que el principal, uno de los principales objetos de estudio de la disciplina. Basta mencionar el abordaje de Tucídides y su "Historia de la Guerra del Peloponeso", "El Príncipe", de Maquiavelo, o "Leviatán", de Thomas Hobbes. Más recientemente, el siglo XX vio nacer obras como "La Crisis de los 20 años (1919 – 1939)" de Edward H. Carr, "Política entre las Naciones" de Hans Morgenthau, y "El hombre, el Estado y la guerra" de Kenneth Waltz, entre otros.

Desde una perspectiva realista, estos autores teorizan sobre las causas de las guerras. El poder es el elemento fundamental en sus explicaciones. Ya sea por incrementarlo o porque los demás lo incrementan generando temor, el poder se encuentra al centro del análisis realista de las relaciones internacionales y los factores que lo otorgan son de diversa índole: la geografía, los recursos naturales, la economía, lo militar, la política, lo psicológico, la tecnología y la información (Vargas, 2011).

La Geopolítica, como campo de estudio, brinda una perspectiva teórica sobre cómo los factores geográficos (espacio, recursos, territorio) determinan las relaciones de los Estados en la arena internacional, desde la pelea por los recursos naturales, los mares, el petróleo, las rutas comerciales y, en pleno siglo XXI, el ciberespacio.

El presente artículo tiene el objetivo de hacer un análisis teórico y documental sobre la Geopolítica y el ciberespacio, así como de las dinámicas de poder que suceden en esta dimensión que, con el acelerado avance de las tecnologías de la información, incrementa su complejidad al mismo tiempo en que se expande el ámbito de acción de los Estados en la lucha por su supervivencia, el control y la seguridad.

La primera parte realizará un breve recorrido por la Geopolítica como disciplina y la importancia que tiene hoy en relación con el estudio del espacio. Posteriormente, abordaremos el concepto del *ciberpoder*, las estrategias para incrementarlo y el estado actual, según estudios, sobre las potencias que mayormente lo acumulan.

El tercer apartado hará referencia a la infraestructura del ciberespacio, su conformación y, más relevantemente, el control de dicha infraestructura y lo que ello implica. Finalmente, el sexto apartado presentará las conclusiones.

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

2 GEOPOLÍTICA Y PODER: EL CONTROL DEL ESPACIO

El espacio es, y ha sido por mucho tiempo, motivo de conflicto en la arena internacional. La lucha por territorio, los recursos, las rutas marítimas, los derechos de paso o la delimitación de las fronteras con motivo de seguridad han determinado las dinámicas que caracterizan las relaciones entre los Estados hasta el día de hoy.

La Ciencia Política, la Geografía, la Antropología, y un cúmulo de disciplinas dentro de las Ciencias Sociales han abordado el espacio territorial y su estudio desde distintas perspectivas, sin embargo, es la Geopolítica la que, de manera más precisa, estudia la relación entre el espacio, el poder y la influencia de la geografía en las relaciones internacionales.

La Geopolítica se considera una rama de la Ciencia Política y a menudo es confundida con la Geografía Política. Incluso, existen autores que las utilizan como sinónimos. No obstante, para efectos de este capítulo, haremos una diferencia entre ambas. Mientras que la Geografía Política está enfocada desde lo doméstico y estatal, la Geopolítica tiene una perspectiva más bien sistémica, enfocada al estudio de la influencia de los factores geográficos en las relaciones interestatales, como lo indicaría el geógrafo Kjellen, acuñador del término en 1899.

Hans Weigert, citado por Cuéllar Laureano (2012), define Geopolítica como la disciplina científica que trata de la dependencia de los hechos políticos con relación al territorio y establece como su objetivo el proporcionar las armas para la acción política, y los principios que sirven de guía en la vida política.

Aunque el concepto se define hasta finales del siglo XIX, el estudio de la influencia de la geografía en el escenario internacional en realidad viene desde mucho antes, pues su nacimiento coincide principalmente con dos factores: los descubrimientos del siglo XV y el surgimiento de la Geografía como una disciplina académica. De la combinación entre el colonialismo y la cartografía surgiría la Geopolítica imperialista. De ahí que la disciplina esté asociada con términos como el poder, la conquista, el control de recursos para asegurar la supervivencia, especialmente con el imperialismo británico y estadounidense.

Mackinder, creador de la teoría del *Heartland*, identifica incluso tres épocas dentro de lo que él denomina “la historia geopolítica”, en donde la época precolombina se

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

caracteriza por las invasiones desde Asia hasta Europa; la colombina, por el expansionismo europeo a través de los mares, y la poscolombina, en donde el espacio se "cierra", no hay más hacia donde expandirse, e inicia la pelea por la eficiencia relativa. En cada una de estas "épocas", Mackinder identifica factores de poder. En la precolombina, el uso del caballo y el camello; en la colombina, buques de navegación y transporte marítimo, y en la poscolombina, las vías ferroviarias.

El siglo XX traería una mala reputación para la Geopolítica imperialista, dado que sus principios serían utilizados por la Alemania Nazi para justificar sus aspiraciones expansionistas, específicamente con el término *Lebensraum* (espacio vital), que se refería a la lucha de las sociedades por espacio necesario para sobrevivir.

Pero la Guerra Fría y el enfrentamiento entre Estados Unidos y Rusia en un mundo bipolar daría paso a la Geopolítica de la Guerra Fría, caracterizada por la lucha por el control del territorio europeo y del "tercer mundo", con los conflictos en Corea, Vietnam, Cuba y Afganistán; la transferencia del conflicto al espacio exterior, el surgimiento de lo que hoy llamamos Carrera Espacial. El deseo de control trascendía ahora lo territorial y se expandía hacia el espacio fuera de la órbita de la Tierra.

Pero llega la década de 1990 y cae el sistema bipolar. Francis Fukuyama declara el fin de la historia (cabe mencionar, postura que fue altamente criticada); desde su perspectiva, el Liberalismo había triunfado y los valores occidentales se expandirían por todo el globo terrestre. Sin embargo, lo más influyente con el mundo de la posguerra fría no sería la desaparición de la Unión Soviética, sino las revoluciones tecnológicas que introdujeron una nueva dimensión, un espacio que no existía apenas unas décadas atrás y que se convertiría en el nuevo escenario del conflicto: el ciberespacio.

El ciberespacio se define como "un dominio global formado por las tecnologías de la información y la comunicación (TIC) y otros sistemas electrónicos, su interacción y la información que es almacenada, procesada o transmitida por estos" (Argumosa, 2022, p.68). Se presenta como "un área virtual prácticamente libre de restricciones" (Rubio Piñeiro, 2022, p.44). Este espacio digital está integrado por cuatro niveles: el físico, el lógico, el de los datos y el social. El primer nivel se refiere a los cables que permiten el flujo de datos e información. El segundo describe las reglas y procedimientos que lo hacen funcional. El tercero alude a todos los datos contenidos en las comunicaciones,

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

como correos electrónicos y el contenido de las páginas de internet. El último nivel, el cuarto o social, es el que convierte al ciberespacio en un espacio de interacción y comunicación (Riordan, 2022).

Según Riordan (2022) el espacio geopolítico es tanto el contexto socioespacial de la función política como los actores sociales, los roles y las dinámicas espaciales que constituyen el escenario. Si bien Rivas (2021) considera que Geopolítica tiene cuatro ámbitos de aplicación tradicional (tierra, mar, aire y espacio exterior), también hace énfasis en la ampliación de la geopolítica en tiempos modernos, específicamente en el siglo XXI, donde se ha experimentado el uso del internet como una práctica masificada que forma parte de la vida cotidiana de las personas, por lo que se ha convertido en un área de interés también para los Estados. Esta nueva dimensión, donde el ciberespacio forma parte de las áreas de aplicación del poder "establece un nuevo orden en la estrategia de poder, en la que los Estados- Nación de los países centrales ejercen el planeamiento estratégico geopolítico a nivel internacional" (Prado, 2018, p. 11).

Entonces, se puede entender que la relación entre los conceptos de geopolítica y ciberespacio se representa por medio de la necesidad de los actores estatales, principalmente aquellos desarrollados y con capacidades de protección de su interés nacional, de ejercer su influencia, tomar ventaja y proyectar su poder en la arena internacional por medio del aprovechamiento de oportunidades y amenazas, como el *ciberespionaje* y la exposición de datos confidenciales (Rubio Piñeiro, 2022), en medio de "una acelerada dinámica de desarrollo e innovación en los entornos virtuales" (Rivas, 2021, p. 90).

Bajo este mismo entendimiento, en el ciberespacio existe el concepto *Traceroute*. De acuerdo con Prado, el *Traceroute* es

…una consola de diagnóstico que permite seguir la pista de flujo de información que se recorre entre los extremos de comunicación de dos computadoras y produce un reporte de los lugares por los que pasó la conexión y el tiempo estimado del recorrido. Por lo tanto, ya no son las fronteras sino los *tracerouters*, los trazadores de rutas, a través de los cuales se lleva a cabo un análisis geográfico de los flujos de información, trazando las nuevas fronteras del ciberespacio y confeccionando un nuevo mapa de jerarquías de poder. Dicho esto, la reducción de la geografía a la cartografía no debe continuarse con

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

una reducción de la geografía a la política y sus necesidades culturales, sino que la geografía puede hoy extenderse a las conexiones cibernéticas de las realidades sociales, y a partir de esta nueva relación elaborar un análisis político del mismo (2018, p. 3).

Debido a procesos como la globalización, que han revolucionado las relaciones internacionales en las últimas décadas, la Geopolítica cibernética adquiere importancia vital en el actuar de los Estados, pues es a partir de ella que éstos deberían "llevar adelante la confección de su mapa de interés, explorar en su análisis los flujos de información, las bases de datos y reconocer por consiguiente, la universalidad de la geografía cibernética y sus nuevas fronteras espaciales" (Prado, 2018, p. 4).

3 CIBERPODER Y EL NUEVO ESCENARIO DEL CONFLICTO

Hans Morgenthau (citado por Pashakhanlou, 2009) menciona que la arena internacional es un escenario competitivo y hostil en el que el poder es el centro de la actividad política a nivel internacional. Para Morgenthau "El poder puede comprender cualquier cosa que establezca y mantenga el poder del hombre sobre el hombre" (Morgenthau, 1965, p. 9). Además, el aspecto material más importante del poder son las fuerzas armadas y de naturaleza militar. (Morgenthau, 1965, p. 186).

En tal sentido del poder, entendido en términos de guerra y fuerza, Clausewitz (citado por Argumosa Pila, 2022, p. 69) afirmaba que "la guerra es un acto de fuerza para obligar al contrario al cumplimiento de nuestra voluntad". Entonces, la fuerza es el medio utilizado por un actor para someter a los demás actores, o enemigos, a cumplir su voluntad. Sin embargo, actualmente los conceptos de fuerza, poder y guerra tienen características y definiciones muy distintas a las utilizadas originalmente en el estudio de las relaciones internacionales. Para Argumosa Pila, el concepto de fuerza incluye no solamente las cuestiones militares, sino también contempla "la economía, la tecnología, la industria, la energía y, por supuesto, el mundo de la cibernética." (2022, p. 69)

Daniel Kuehl (citado por Klimburg & Faesen, 2020, p. 147) define el ciberpoder como "la capacidad de utilizar el ciberespacio para crear ventajas e influir en los

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

acontecimientos en otros entornos operativos y a través de los instrumentos de poder". De igual forma, Joseph S. Nye ofrece orientación al describir el *ciberpoder* como un régimen híbrido único de propiedades físicas (las infraestructuras, los recursos, las normas de soberanía y la jurisdicción) y propiedades virtuales que dificultan el control gubernamental sobre las primeras.

Actualmente el ciberespacio, un espacio sin límites geográficos ni fronteras, representa un nuevo, y aún desconocido, escenario de conflicto. En él se pueden realizar acciones que comúnmente se hacían en espacios físicos y que podíamos experimentar en persona. Hoy por hoy, actores anónimos se hacen presentes en forma de delincuentes, terroristas y espías y afectan un espacio carente de legalidad y en una dimensión de enfrentamientos sistematizados con recursos tecnológicos que presentan diferentes grados de autonomía (Aceves, 2021).

De igual forma, Prado (2018) menciona que estos grados de autonomía generan desigualdades, y estas diferencias “escalan a la cibergeografía, en la cual la herramienta de internet, pese a su acceso rápido e igualitario a los millones de usuarios de todo el mundo, se encuentra jerarquizado. El ciberespacio es un área que encapsula las mismas desigualdades de otrora, pero adaptadas a una dimensión insustancial” (p. 10).

De este modo, y de acuerdo con Rivas (2021) la posición en la que se encuentran los actores estatales en el sistema internacional y en el ciberespacio será entonces fundamental, puesto que el manejo y desarrollo de las tecnologías de conectividad y dispositivos en términos amplios, así como las redes de distribución de internet, supone una influencia directa en otros junto con una potencial oportunidad/amenaza.

Para Riordan (2022) debido a la diferencia en recursos, poder y capacidades de los Estados, existen diferentes formas de entender el ciberespacio. Por ejemplo, para Estados Unidos de América, el ciberespacio representa un recurso que funciona para promover sus propios intereses, pues desde los tiempos de la Guerra Fría, internet representaba una posibilidad de control de ataques y la manera de comunicar temáticas de defensa y seguridad nacional, operando en un espacio que ellos mismos habían creado.

Por el contrario, para Rusia y China, el ciberespacio representa una amenaza que tiene que ser controlada. Para Moscú, la manera de actuar en el ciberespacio tiene dos

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

objetivos principales: el primero nos dice que, al controlar el contenido de internet dentro de sus fronteras, se reducen las amenazas y los riesgos para su política y gobierno, priorizando su soberanía. Por otro lado, el segundo objetivo se centra en el actuar fuera de sus fronteras, en donde se aprovecha el espacio digital para crear inestabilidad, perturbación social, incertidumbre y desinformación.

En China, la red de internet y el ciberespacio representan, más que una oportunidad, una amenaza latente para su sistema político y para el partido comunista. A sabiendas de lo anterior, el gobierno controla y restringe el acceso de sus ciudadanos a internet, pero también utiliza este espacio a su favor para promover sus ideas y su soberanía.

Para la Unión Europea, aunque internet es una creación extranjera (de Estados Unidos), éste no representa un recurso hostil ni una amenaza, sino que entienden el ciberespacio y las herramientas digitales como un medio para mejorar la economía, la educación y el tiempo libre y de recreación. En resumen, ven a este espacio digital como un “espacio colaborativo compartido con los estadounidenses y los demás países occidentales, y el espacio compartido con rivales como Rusia y China, más conflictivo" (Riordan, 2022, p. 77).

Por último, de acuerdo con Fuente Cobo, la Organización del Tratado del Atlántico Norte (OTAN) reconoce que “el uso de la tecnología digital en general y de internet en particular ha convertido el espacio digital en una herramienta indispensable para el funcionamiento de los Estados modernos y le ha otorgado un valor geopolítico.” Por lo tanto, en el 2016 declaró que “debemos ser capaces de operar con tanta efectividad en el ciberespacio como en tierra, mar y aire, para reforzar y ayudar a la postura absoluta de la Alianza en seguridad y defensa.” (Fuente Cobo, 2022, p. 84)

Prado (2018) identifica seis estrategias para acumular poder cibernético. La primera es que en la cibergeografía es de suma importancia la soberanía tecnológica que ejercen los países centrales. El ciberespacio posee centros y periferias y genera una nueva geografía y fronteras entre los Estados. Lo que encubre entonces son las nuevas desigualdades del siglo XXI que muestran nuevas fronteras sedientas de cercanía virtual y con dependencia tecnológica. Un claro ejemplo de un país central es el rol que ocupa Estados Unidos en la geografía cibernética, pues los flujos de información atraviesan las

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

ciudades más importantes del país. Entonces, existe entre los actores estatales una "jerarquía de poderes, específicamente de países centrales con mayor soberanía tecnológica que los periféricos y en donde el conflicto armado internacional podría tener lugar." (p.8)

La segunda es que los países periféricos que delimitan entre sí en sus fronteras geográficas no delimitan entre sí en sus fronteras ciberespaciales. Buzai (2014) explica un ejemplo en este sentido al afirmar que, en Argentina, la velocidad o el tiempo que tarda en establecerse comunicación entre Buenos Aires y ciudades europeas como Oslo, Londres o Mónaco es, en la mayoría de los casos, más corto que el tiempo que se tarda en establecerse comunicación con la mayoría de los países de Latinoamérica.

La tercera es que las Tecnologías de la Información y Comunicación funcionan como una herramienta innovadora para trazar líneas de acción de los Estados. La cuarta es que, con la aparición del ciberespacio, la percepción de incertidumbre frente a supuestas amenazas ha ampliado la esfera de preocupación tanto de la seguridad como de la defensa. La omnipotencia y desmaterialización de internet, como señala Zuazo, N. (2015) citado por Prado (2018) acrecienta la incertidumbre de amenazas, consolida la globalización erosionando las fronteras tradicionales y abre un campo de batalla virtual con efectos adversos en la realidad empírica, librando a una desprotección absoluta a aquellos estados que por periféricos o marginales no logran asegurar sus sistemas informáticos" (p.8).

Por otro lado, de acuerdo con la autora, existe una nueva concepción del término "frontera", pues se habla hoy en día de nuevas fronteras jerarquizadas por el flujo y control de información.

Posteriormente, la autora hace referencia a las Relaciones internacionales "Cibernéticas", dado que el ciberespacio está gestionado por actores de la sociedad civil, el sector privado y, en menor medida, por los gobiernos. Estos últimos, sin embargo, afirman cada vez más su papel en el ciberespacio, lo que lleva a una redistribución del poder en la que los Estados no sólo compiten con otros actores, sino también entre sí. Todos los usuarios del ciberespacio se enfrentan, pues, a una lucha de poder entre los Estados que afecta al sector privado y a la sociedad civil. (Klimburg & Faesen, 2020).

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Asimismo, el *Hard Power* en el ciberespacio es un elemento para considerar. De acuerdo con Klimburg & Faesen (2020) la manifestación del poder duro del ciberespacio es la capacidad de vulnerar la disponibilidad, confidencialidad e integridad de los datos. Esto puede lograrse mediante la denegación de servicios (DDoS), mediante ciberespionaje o mediante diversos métodos diseñados para influir en la integridad de los datos (por ejemplo, la inserción de malware destructivo por diversos medios). Así pues, es lógico que la capacidad de los Estados para infligir daños de efecto cinético en el ciberespacio requiera (en diversos grados) la capacidad de reunir información de inteligencia. (Klimburg & Faesen, 2020)

Finalmente, el anonimato que ofrece el ciberespacio es una característica importante. Para Aguilar (2010, p. 181) citado por Prado (2018) la comprensión del ciberespacio no puede darse en términos de espacio, sino de dimensión, pues se trata de "un dominio que no es físico sino virtual" y el mismo no cuenta con una "locación física específica". Así, este espacio digital representa una ventaja para influir y dominar de manera anónima, pues "mientras que el planeamiento estratégico militar utiliza armas convencionales y los cuerpos e instrumentos militares son posibles de ser rastreados, contrariamente el malware (*malicious software*) informático no es fácilmente detectable" (p.9).

4 ¿QUIÉNES CONCENTRAN MAYOR PODER CIBERNÉTICO?

En los últimos años, se han realizado numerosos intentos para identificar a las potencias estatales en el ciberespacio. Estas investigaciones, como las realizadas por el *Belfer Center* de Harvard y el Instituto Internacional de Estudios Estratégicos (IISS, por sus siglas en inglés), han analizado las capacidades, tendencias y características que ejercen los estados en esta área para conocer el dominio, las ventajas y las debilidades que tienen sobre los demás.

El *Belfer Center de la Harvard Kennedy School* mide las capacidades cibernéticas de los países utilizando el Índice de Poder Cibernético Nacional (NCPI, por sus siglas en inglés), el cual se basa en siete objetivos principales: Vigilancia y seguimiento de grupos nacionales; Fortalecimiento y mejora de las ciberdefensas nacionales; Controlar y

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

manipular el entorno de la información; Recogida de información extranjera para la seguridad nacional; Obtención de beneficios comerciales o mejora del crecimiento de la industria nacional; Destrucción o inutilización de la infraestructura y las capacidades de un adversario; y, Definición de normas y estándares técnicos internacionales. Los resultados, que fueron publicados en el año 2020, muestran que las potencias cibernéticas más completas son, del 1º al 10º: Estados Unidos, China, Reino Unido, Rusia, Países Bajos, Francia, Alemania, Canadá, Japón y Australia (The Economist, 2020).

Tabla 1
Países con mayor poder cibernético

Países con mayor Poder Cibernético	Países con mayor Poder Cibernético de Ataque	Países con mayor Poder Cibernético de Defensa
1. Estados Unidos de América	1. Estados Unidos de América	1. China
2. China	2. Reino Unido	2. Francia
3. Reino Unido	3. Rusia	3. Países Bajos
4. Rusia	4. China	4. Estados Unidos de América
5. Países Bajos	5. España	5. Canadá
6. Francia	6. Israel	6. Japón
7. Alemania	7. Alemania	7. Suecia
8. Canadá	8. Irán	8. Reino Unido
9. Japón	9. Países Bajos	9. Suiza
10. Australia	10. Francia	10. Alemania

Fuente: Adaptado de *The Economist* (2020)

De acuerdo con el análisis de *The Economist* (2020), no es casualidad que los Estados Unidos de América sea el primer lugar en capacidades cibernéticas, dado que el presupuesto asignado para la seguridad en dicho rubro para el año fiscal 2020 superó los $ 17 mil millones de dólares y la Agencia de Seguridad Nacional (NSA), su agencia de inteligencia de señales (SIGNT), probablemente obtenga más de $ 10 mil millones. China, en segundo lugar, ha incrementado sus actividades de *ciberespionaje* comercial en el extranjero y un control férreo de Internet en casa. Gran Bretaña, cuyo Centro Nacional de Seguridad Cibernética ha evitado más de 1,800 ciberataques desde su creación en 2016, ocupa el tercer lugar. Gran Bretaña está estableciendo actualmente una Fuerza Cibernética Nacional ofensiva integrada conjuntamente por espías y

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

soldados. Rusia, cuyos espías interfirieron en las últimas elecciones de Estados Unidos, ocupa el cuarto lugar.

Por su parte, el IISS desarrolló una metodología para evaluar las capacidades cibernéticas de los Estados y cómo contribuyen al poder nacional. El estudio se enfocó en un conjunto de países específicos: Estados Unidos de América, Reino Unido, Canadá, Australia, Francia, Israel, Japón, China, Rusia, Irán, Corea del Norte, India, Indonesia, Malasia y Vietnam.

El organismo realizó las evaluaciones dividendo las capacidades de los Estados en siete categorías: estrategia y doctrina; gobernanza, comando y control; capacidad básica de *ciberinteligencia*; *ciberempoderamiento* y dependencia; ciberseguridad y resiliencia; liderazgo mundial en asuntos del ciberespacio, y capacidad cibernética de ofensiva.

Este informe arroja resultados en torno a cada una de las categorías, entre los que destacan, por ejemplo, que todos los países evaluados, incluso los más poderosos, han batallado para dar forma a políticas públicas para el ciberespacio, ya sea con el propósito de aprovechar nuevas oportunidades o de defenderse de nuevas amenazas El dinamismo del entorno cibernético ha obligado a los países más avanzados a revisar constantemente sus documentos estratégicos. Por lo tanto, puede afirmarse que prácticamente todos los países siguen en las primeras etapas de adaptación a nuevas ciberestrategias.

Tan es así, que al sector público ha rebasado al sector privado, el cual ha sido impulsado por el consumidor. En varios países, la industria cibernética avanza a tal velocidad que cuenta con capacidades de vigilancia e inteligencia más eficaces que las gubernamentales, lo que arroja una advertencia importante con respecto al rumbo que está tomando nuestra sociedad.

El reporte afirma también que algunos gobiernos conciben hoy el ciberespacio como una arena de competencia existencial, aún y cuando intenta promover la colaboración internacional en la materia. La falta de transparencia en esta dimensión impide un mayor involucramiento de la gobernanza internacional, aunque existan alianzas como *Five Eyes* (Cinco ojos), quienes han desarrollado mecanismos eficaces para la detección de amenazas terroristas en línea después del 9/11, pero que han sido

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

altamente cuestionados, al igual que otros mecanismos para recabar información de inteligencia para generar una acción cibernética ofensiva. Estados Unidos y el Reino Unido se encuentran entre los países donde la necesidad de una mayor transparencia en materia de ciberseguridad ha sido reconocida. Ha habido varias iniciativas para mejorar la apertura, incluyendo un mayor intercambio de datos sobre amenazas y vulnerabilidades con la industria y el público.

Otra problemática identificada es que las capacidades y la resiliencia cibernética futura de muchos estados depende de la infraestructura física del internet, cómo está construida y de quién es. Más adelante, el presente artículo desarrolla un apartado en donde se explica precisamente cómo se compone hoy dicha infraestructura.

La lucha por controlar el espacio cibernético transciende lo tecnológico y la infraestructura en el sentido de que la sociedad en sí es un elemento de la seguridad cibernética. Los países más desarrollados han estado presionando para que exista una mayor colaboración para compartir información entre los sectores público y privado, involucrando a la academia, así como a las asociaciones civiles e instancias militares. Por supuesto, existen diferentes enfoques para lograr lo anterior: regímenes más autoritarios como Rusia, China e Irán, ejercen un control vertical sobre lo que entra o no en su espacio cibernético, y apuestan por mantener su “soberanía” en él. Por otro lado, los países con sistemas más democráticos apuestan más por un enfoque de gobernanza, innovación y protección de los datos de los ciudadanos.

Dicha lucha también puede reflejarse en las inversiones financieras para desarrollar capacidades cibernéticas. Aunque éstas son difíciles de medir, los estudios sugieren que las inversiones de los

Estados Unidos, China y Rusia son los más grandes. Varios estados se han movido decisivamente para transformar sus estrategias, doctrinas y estructuras militares para reconocer tanto las oportunidades como las amenazas creadas por el ciberespacio, en donde las predicciones indican que se librará la guerra futura.

Finalmente, el estudio indica la inteligencia cibernética es la base principal del *ciberpoder*. Esto quiere decir que la capacidad de cualquier país para emprender acciones defensivas u ofensivas en el ciberespacio depende fundamentalmente de su conocimiento del entorno digital, el cual puede construirse a partir de la información

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

recopilada de los sectores público y privado. En este rubro destacan países como Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda (que operan colectivamente gracias a su alianza de inteligencia "Five Eyes" o Cinco Ojos); Israel y Francia (socios de los anteriores) y China y Rusia.

De acuerdo con Rizzi (2022), atendiendo a los resultados presentados por los estudios descritos en los párrafos anteriores, los expertos coinciden en que Estados Unidos representa el poder dominante, pues tiene diversas y claras ventajas cibernéticas frente a los demás estados. Junto a él, China asciende a los primeros puestos en poderío cibernético, pues su comprensión del espacio digital lo coloca a la par de Estados Unidos. Diferentes países europeos, como Reino Unido y Países Bajos, también son actores relevantes en cuanto a poder cibernético significa, sin embargo, tienen limitaciones y dificultades debido a la supranacionalidad de la Unión Europea. Además, Rusia emerge como potencia cibernética agresiva, con grandes capacidades de ofensa digital.

Sin embargo, para otros autores, como Jelle van Haaster (2016), de la Facultad de Ciencias Militares de la Academia de Defensa de los Países Bajos, no puede existir una conclusión general o afirmación verídica de quiénes son los actores con poder cibernético y cuáles son los débiles en el sistema internacional, pues el ciberpoder depende de dimensiones contextuales y temporales, entonces existen un sinfín de contingencias como para englobarlas en un análisis general.

5 LA INFRAESTRUCTURA CIBERNÉTICA

Las tecnologías de la comunicación (TIC) y la información han evolucionado de tal manera que dan respuesta a la necesidad de almacenar, difundir y codificar la información. La complejidad de su evolución se refleja hoy no solamente en la cantidad de información que fluye, sino en la fragmentación de los dispositivos a través de los cuales la sociedad tiene acceso a ella, como las computadoras, los teléfonos inteligentes y las tabletas. De acuerdo con Romero (2019), hacia el 2017, los suscriptores de teléfonos celulares a nivel mundial eran del 103% de la población, de los cuales el 60% correspondía a celulares inteligentes. Asimismo, apenas el 47.6% de las casas contaba

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

con una computadora en casa, sin embargo, si se analiza el dato diferenciado por países desarrollados y en desarrollo, del primer grupo el 82% de las casas tenía computadora, mientras que en los países en desarrollo era solo el 35.5%.

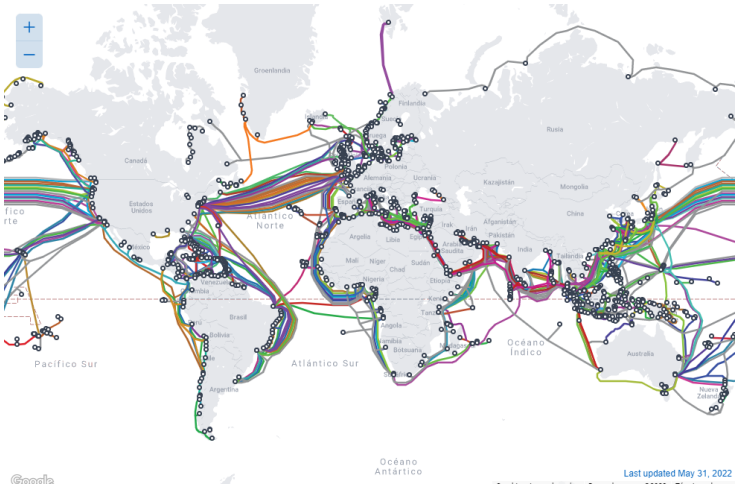
Pero ¿qué es en realidad el internet? De acuerdo con Gonzalo (2017), el internet se compone de infraestructura que comprende una gran variedad de componentes, como de centros de datos, servidores, dispositivos de almacenamiento, *routers*, cables, repetidores, módems, entre otros. Esta red global utiliza un lenguaje común o protocolo que se conoce como TCP/IP. Más allá de ser una nube, el internet es "un despliegue de equipos físicos remotos y programas informáticos que controlan distintos aspectos de su arquitectura y trabajan para enviar y recibir información a distintos sistemas" (par. 9).

El internet, entonces, no necesariamente una dimensión completamente abstracta, porque tiene componentes tangibles, y estos se encuentran en el océano. Como lo explica Gonzalo (2017), "suelen ser líneas con múltiples cables de fibra óptica, y la mayor parte está bajo el agua. Nuestra imagen de la nube es sólo una metáfora visual porque internet en realidad está en los océanos: el 99% del tráfico de internet circula debajo del mar" (par. 12).

Por lo tanto, si quisiéramos ver de manera gráfica cómo se ve la infraestructura de internet en el mundo, lo que observaremos es una amplia red de cableado que cruza los océanos y que conecta los territorios (ver imagen 1). Actualmente, existen más de 400 cables de fibra óptica que forman parte de la infraestructura del internet.

Imagen 1

Mapa de cables submarinos



REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Fuente: TeleGeography (2021). Disponible en: https://www.submarinecablemap.com/

Como se observa en la Imagen 1, estos cables tocan tierra en centros de datos, los cuales son básicamente edificios con servidores y con sistemas de seguridad, y que pueden tener uno o varios dueños. Gonzalo (2017), explica que "el espacio físico que dota de infraestructura a internet puede ser propiedad de una o distintas compañías, que pueden dar servicios a otras empresas que operan con él o entre sí" (par. 17). Los centros de datos son como centros de colocación.

Los 15 proveedores de colocación de centros de datos más grandes del mundo poseen aproximadamente el 50% del mercado. La mitad restante está extremadamente fragmentada, lo que significa que seguirá una mayor consolidación (Sverdlik, 2021). De las 15 compañías, siete son estadounidenses, cinco son chinas, dos son japonesas y una británica (Ver Tabla 1).

Tabla 1
Empresas que concentran la mitad del mercado de proveedores de centros de datos

Empresa	Origen	% del mercado global
1. Equinix	Redwood City, California, Estados Unidos de América	11%
2. Digital Realty Trust	Austin, Texas, Estados Unidos de América	7.6%
3. China Telecom	Beijing, China	6.1%
4. NTT GDC	Tokio, Japón	4.3%
5. China Unicom	Beijing, China	4.2%
6. China Mobile	Beijing, China	2.1%
7. CyrusOne	Dallas, Texas, Estados Unidos de América	1.9%
8. KDDI Telehouse	Tokio, Japón	1.9%
9. GDS	Shanghai, China	1.6%
10. Global Switch	Londres, Reino Unido	1.4%
11. 21Vianet	Beijing, China	1.4%
12. CoreSite	Denver, Colorado, Estados Unidos de América	1.3%
13. Cyxtera	Coral Gables, Florida, Estados Unidos de América	1.2%
14. Lumen (formerly CenturyLink)	Monroe, Louisiana, Estados Unidos de América	1.1%
15. Flexential	Charlotte, North Carolina, Estados Unidos de América	1.1%

Fuente: elaboración propia con información de Sverdlik (2021)

REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL
unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Adicionalmente, existen puntos de intercambio de tráfico, denominados IXP, que se definen como una infraestructura técnica esencial donde las redes se unen para conectarse e intercambiar tráfico de Internet. Algunos de los tipos de redes que se conectan para intercambiar tráfico son: proveedores de servicios de Internet (ISP), operadores móviles y redes de entrega de contenido (CDN) como Google, Baidu, Akamai y Facebook. Los IXP permiten que redes locales intercambien información de manera eficiente en un punto común dentro de un país, sin la necesidad de intercambiar el tráfico de Internet local en el extranjero.

Ahora, las empresas que concentran el mercado de los servidores con espacio en la nube son distintas, y también son pocas. A febrero de 2021, AWS, Azure, Google Cloud y Alibaba ostentan el 67% de la cuota de mercado global. Amazon Web Services (Estados Unidos de América) tuvo el mayor porcentaje con un 32%, seguido de Microsoft Azure (Estados Unidos de América) con un 20%. Google Cloud (Estados Unidos de América) ostenta el 9%, mientras que Alibaba Cloud (China) representó el 6% (Data Center Market, 2021).

Como ha podido observarse con los datos anteriores, la infraestructura del internet, que es fundamental para su funcionamiento, está concentrada principalmente en dos polos de poder: China y Estados Unidos. La guerra comercial que ambas potencias han protagonizado en la última década simplemente se refleja en la realidad de la infraestructura para el intercambio de información.

6 CONCLUSIONES

El ciberespacio como nuevo escenario del conflicto internacional obliga a la Geopolítica a expandir su objeto de estudio hacia una nueva dimensión que incrementa su complejidad cada vez más, de forma más rápida y con más actores involucrados. Los gobiernos han debido ajustarse constantemente, tanto en sus estrategias como en sus marcos jurídicos, al crecimiento del ciberespacio, sin embargo, han sido las empresas las

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

que mejor han podido adaptarse y quienes juegan un papel preponderante en el control de esta nueva dimensión.

Por lo anterior, los gobiernos deben buscar mayor interacción y gobernanza con el sector privado, las universidades y la sociedad civil, para evitar que la infinitud del ciberespacio los sobrepase y sea más difícil garantizar su supervivencia y la protección de sus poblaciones. La protección de la frontera física no es suficiente, y no es ni siquiera porque ésta se haya erosionado debido a la globalización, sino porque, en el ciberespacio, las fronteras apenas si se están formando. Están si acaso más claras en los países que controlan más autoritariamente la información de internet que entra o no a sus países, pero aún así, dicho control requiere de grandes esfuerzos.

Aunado a lo anterior, la parte "física" del internet, es decir, la infraestructura, no está controlada por los países, sino por el sector privado, como se han mencionado anteriormente. El Estado no controla estos canales en su totalidad, tampoco controla la nube que almacena la información, aunque tenga alguna participación. Todo ello lo hacen las empresas, en su mayoría estadounidenses, pero con las chinas por detrás.

En términos más tradicionales, el ciberespacio internacional podría entenderse también como ese espacio anárquico, en otra dimensión, en el que los actores buscan sobrevivir, acumular poder y defender el interés nacional, sin embargo, quizá la diferencia en este caso es que, en este ciberespacio, los Estados no han llevado tradicionalmente la ventaja ni la primicia a la hora de definir la forma de interactuar, y entonces actores como las empresas y la sociedad civil ganan mayor influencia. Un constructivista en Relaciones Internacionales incluso argumentaría que es el internet el que ha dado mayor poder de influencia a la sociedad civil para influir en el actuar de los Estados. Y tal vez es por ello que Estados como Rusia son más propensos a tolerar que *hackers* o justicieros cibernéticos agredan a los sistemas de otros Estados o de empresas en nombre del orgullo nacional.

El ciberespacio es, en efecto, una nueva dimensión geopolítica, pero no está desconectada del sistema internacional. Más bien, forma ahora parte de él y lo hace todavía más complejo, con más actores, más flujo de información y mayor rapidez. Es de notarse que replica muchos de los patrones antes identificados dentro del sistema por

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Morgenthau o Waltz, incluso de autores más liberales, como Nye: acumulación de poder, jerarquía, interdependencia.

En realidad, muchas de las herramientas utilizadas en la dimensión física para garantizar la supervivencia y seguridad de los Estados en un sistema anárquico se utilizan también en el ciberespacio, como el ciberespionaje, la ciberinteligencia, los ciberataques, la cibervigilancia. La generación de inteligencia a través del ciberespacio es una herramienta imprescindible para los servicios de seguridad nacionales de los estados más poderosos. Pero todo lo anterior con nuevas formas de "frontera".

Finalmente, la geopolítica en el ámbito del ciberespacio replica también la distribución del poder económico y comercial. No es sorpresa que Estados Unidos de América sea el líder en la acumulación de capacidades cibernéticas, y que las amenazas a su estabilidad vengan de sus enemigos con menores capacidades, pero con mayor impulso para manifestar su poder, como lo son Rusia o incluso Corea del Norte. Tampoco es sorpresa que China sea el segundo lugar en capacidades cibernéticas, replicando su lugar como segunda economía más grande del mundo.

REFERENCIAS

Aceves, M. D. (2021). *2021: geopolítica, gobernanza y ciberseguridad*. Foreign Affairs Latinoamérica. Disponible en: https://revistafal.com/2021-geopolitica-gobernanza-y-ciberseguridad/

Argumosa Pila, J. (2022). El impacto del ciberespacio en las guerras del siglo XXI *EJÉRCITO, Revista del Ejército de Tierra Español*, *Año LXXXIII*(972), 68–71. https://publicaciones.defensa.gob.es/ejercito-de-tierra-espa-ol-972-revistas-papel.html

Voo, J., Hemani, I., Jones, S., DeSombre, W., Schwarzenbach, A., Cassidy, D., & Belfer Center, Harvard Kennedy School. (2020). *National Cyber Power Index 2020*. Belfer Center for Science and International Affairs. Disponible en: https://www.belfercenter.org/publication/national-cyber-power-index-2020

Buzai, G.D. (2014). Fronteras en el ciberespacio: el nuevo mapa mundial visto desde Buenos Aires (Argentina). *Cuadernos de Geografía.* Vol.23. Bogotá. Colombia. pp 85- 92.

Data Center Market (2021). AWS, Azure, Google Cloud y Alibaba ostentan el 67% de la cuota de mercado global. Recuperado de: https://www.datacentermarket.es/tendencias-

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

tic/noticias/1123667032809/aws-azure-google-cloud-y-alibaba-ostentan-67-de-cuota-de-mercado-global.1.html

Echeberría, R. (2020). Infraestructura de Internet en América Latina. Comisión Económica para América Latina y El Caribe. Naciones Unidas: Santiago.

Klimburg, A. & Faesen, L. (2020). A Balance of Power in Cyberspace. En Broeders, D. & van der Berg, B. (1st. Ed) *Governing Cyberspace: Behavior, Power and Diplomacy* (pp. 145–172). Disponible en: https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf

International Institute for Strategic Studies (IISS). (2021). *Cyber Capabilities and National Power: A Net Assessment*. Disponible en: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

Marilín, G. (2021). Cómo es la infraestructura de Internet y quiénes son sus dueños. Recuperado de: https://www.newtral.es/infraestructura-internet-duenos/20210707/

Morgenthau, H. (1965) *Politics Among Nations*. New York: Alfred A. Knopf.

Morgenthau, H. (1963) *La lucha por el poder y por la paz*, ed. Sudamericana, Buenos Aires.

Pashakhanlou, A. H. (2009). *Comparing and Contrasting Classical Realism and Neorealism*. E-International Relations. Disponible en: https://www.e-ir.info/2009/07/23/comparing-and-contrasting-classical-realism-and-neo-realism/

Prado, B. (2018) Geopolítica del ciberespacio: hacia el *heartland* cibernético. *Geografía y Sistemas de Información Geográfica (GeoSIG).* 10(10) Sección I: Artículos, p. 1-13 Disponible en: https://revistageosig.wixsite.com/geosig

Riordan, S. (2022). La Geopolítica del Ciberespacio. *EJÉRCITO, Revista del Ejército de Tierra Español*, *Año LXXXIII*(972), 84–91. https://publicaciones.defensa.gob.es/ejercito-de-tierra-espa-ol-972-revistas-papel.html

Rivas, S. M. (2021) El Ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos, *Revista Relaciones Internacionales*, (III), pp. 89–107. Disponible en: https://revistas.ues.edu.sv/index.php/reinter/article/view/2069

Rizzi, A. (2022). *¿Quién tiene más ciberpoder? Una radiografía de las capacidades de EE UU, China, Rusia y otras potencias*. El País. https://elpais.com/internacional/2022-01-30/quien-tiene-mas-ciberpoder-una-radiografia-de-las-capacidades-de-ee-uu-china-rusia-y-otras-potencias.html

unicuritiba
Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Romero, O. (2019). Telecomunicaciones y dependencia en América Latina: retos para la integración autónoma. *Controversias y Concurrencias Latinoamericanas*, 11(19), 137-155.

Rubio Piñeiro, G. J. (2022). Redes Sociales, Geopolítica y Poder. *Redes Sociales, Geopolítica y Poder*, *1*(1), 43–58. https://doi.org/10.56221/spt.v1i1.6

Sverdlik, Y. (2021). 2021: These are the World's Largest Data Center Colocation Providers. Data Center Knowledge. Recuperado de: https://www.datacenterknowledge.com/archives/2017/01/20/here-are-the-10-largest-data-center-providers-in-the-world

The Economist (2020). A new global ranking of cyber-power throws up some surprises. Disponible en: https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises

UNCTAD (2021). Informe sobre tecnología en información 2021. Disponible en: https://unctad.org/system/files/official-document/tir2020overview_es.pdf

van Haaster, J. (2016). *Assessing Cyber Power*. Disponible en: https://ccdcoe.org/uploads/2018/10/Art-01-Assessing-Cyber-Power.pdf

Vargas (2011). Motivaciones y causas de la guerra: una reinterpretación del neorrealismo de Stephen Van Evera. *Revista Estudios en Seguridad y Defensa* 6(12), 51-57.

World Economic Forum (2020). Mapping TradeTech: Trade in the Fourth Industrial Revolution. Disponible en: https://www3.weforum.org/docs/WEF_Mapping_TradeTech_2020.pdf