La ciberdiplomacia en relación con el ciberpoder: mecanismos y estrategias para la consecución de intereses nacionales

Cómo citar este artículo [Chicago]: Realpe Díaz, Milena Elizabeth. "La ciberdiplomacia en relación con el ciberpoder: mecanismos y estrategias para la consecución de intereses nacionales". *Novum Jus* 18, núm. 2 (2024): 279-304. https://doi.org/10.14718/NovumJus.2024.18.2.11

Milena Elizabeth Realpe Díaz

Código: 1312417775 • Autor: istockphoto.com

https://doi.org/10.14718/NovumJus.2024.18.2.11

La ciberdiplomacia en relación con el ciberpoder: mecanismos y estrategias para la consecución de intereses nacionales*

Milena Elizabeth Realpe Díaz**
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Recibido: 17 de octubre de 2023 **| Evaluado:** 30 de enero de 2024 **| Aceptado:** 8 de febrero de 2024

Resumen

El objetivo del presente artículo es analizar las dinámicas que acontecen en el ciberespacio e identificar aquellas relevantes para el sistema internacional, principalmente las que constituyen amenazas a la estabilidad de las naciones por cuenta de la puja por el poder en la geopolítica contemporánea. En este contexto, en el que la OTAN decide reconocer desde el año 2016, el ciberespacio como un dominio, se hace necesario incorporar una nueva herramienta llamada ciberdiplomacia, como parte de la diplomacia científica, en relación con el ciberpoder de un país para alcanzar los intereses nacionales. La metodología empleada obedece a una revisión sistemática de diversos estudios primarios o individuales, se incorporó literatura gris y la interpretación y comprensión de la investigadora, por medio de un análisis comparado sobre acepciones de la ciberdiplomacia con sus categorías. Se destaca la importancia de este concepto, el cual bien puede considerarse un neologismo en evolución, de creciente arraigo en los temas propios del sistema internacional y el ciberpoder de un Estado.

Palabras clave: ciberespacio, ciberpoder, ciberdiplomacia, geopolítica, sistema internacional

* Este artículo presenta los resultados del proyecto de investigación "Tecnologías disruptivas, logística global y seguridad y defensa en el ciberespacio", vinculado a la línea de investigación de Ciberseguridad y Ciberdefensa, del grupo de investigación "Ciberespacio, Tecnología e Innovación," de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado como 'C' por Minciencias y con código de registro COL0181179. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

** Ingeniera de sistemas, Universidad Cooperativa de Colombia; especialista en Seguridad de redes de computadores, Universidad Católica de Colombia; especialista en Seguridad física y de la informática, Escuela de Comunicaciones del Ejército; especialista en Seguridad de la Información, Universidad de los Andes; magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra; magíster en Seguridad de la Información, Universidad de los Andes; PhD(c) en Estudios estratégicos, seguridad y defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto". Teniente coronel del Ejército Nacional de Colombia. https://orcid.org/0000-0003-4345-6182 - Contacto: milena.realpe@esdeg.edu.co

https://doi.org/10.14718/NovumJus.2023.17.2.11

Cyber Diplomacy in Cyber Power: Mechanisms and Strategies for Furthering National Interests

Milena Elizabeth Realpe Díaz
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Received: October 17, 2023 **| Evaluated:** January 30, 2024 **| Accepted:** February 08, 2024

Abstract

This article aims to examine the dynamics in cyberspace and identify those relevant to the international system, mainly those threatening nations' stability due to the struggle for power in contemporary geopolitics. In this context, where even NATO has recognized cyberspace as a domain since 2016, it is necessary to introduce a new diplomatic tool called cyber diplomacy as part of scientific diplomacy in a country's cyber power to advance its national interests. The methodology used is a systematic review of various primary or individual studies. Gray literature and the interpretation and understanding of the researcher are incorporated through a comparative analysis of the meanings of cyber diplomacy and its categories. The importance of this concept is stressed as it can well be considered an evolving neologism with increasing roots in the issues of the international system and the cyber power of any State.

Keywords: cyberspace, cyber power, cyber diplomacy, geopolitics, international system

Introducción

La llegada de Internet y las tecnologías digitales ha tenido un profundo efecto en la sociedad, al unir personas y empresas en todo el mundo, lo que ha dado lugar al aumento significativo de desafíos y problemas adicionales en términos de seguridad y estabilidad global. La progresión del entorno cibernético ha conducido a la creación de métodos novedosos de enfrentamiento, que engloban actividades como el espionaje digital, la delincuencia cibernética, ataques a infraestructuras críticas digitales y el hacktivismo, entre otras[1]. Los avances en la tecnología actual han habilitado a las personas para adentrarse en una época luminosa de información; sin embargo, las carencias en la seguridad digital traen consigo posibles peligros y amenazas ambiguas[2]. Por su parte, la trasformación digital y la expansión de las tecnologías de la información, la comunicación y la operación han llevado a un uso cada vez más importante de Internet[3].

Este nuevo ambiente tecnológico ha traído consigo un sinnúmero de oportunidades, pero también retos y desafíos asociados a la estabilidad económica y social, así como a la seguridad y a la defensa nacionales. Así las cosas, las recientes amenazas han mostrado la urgencia de fortalecer la colaboración internacional, con el fin de abordar estos obstáculos y asegurar la seguridad y estabilidad del entorno digital global[4]. Si bien es cierto que la diplomacia convencional tiene la función de crear ventajas comunes mediante el diálogo, para asegurar un espacio digital seguro con la ciberdiplomacia, los actores en el ciberespacio (gobiernos, organizaciones, corporaciones, sector privado y sociedad civil) deberán colaborar, negociar y desarrollar capacidades cibernéticas.

Las dinámicas tecnológicas contemporáneas, las preocupaciones del cambio climático, las pandemias mundiales y la economía digital, entre otros, podrían considerarse importantes desafíos diplomáticos[5]. En las últimas dos décadas, para

1 André Barrinha y Thomas Renard, "Cyber-diplomacy: The Making of an International Society in the Digital Age", *Global Affairs* (2017): 1-16, https://doi.org/10.1080/23340460.2017.1414924

2 Jiangxing Wu, "Cyberspace Endogenous Safety and Security", *Engineering* 15 (2022): 179-185, https://www.sciencedirect.com/science/article/pii/S2095809921003179

3 Johan Eriksson y Giampiero Giacomello, "Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty" en *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, ed. Myriam Dunn Cavelty y Andreas Wenger (Nueva York: Routledge, 2022), 95-107.

4 Kenneth Geers, "Cyberspace and the Changing Nature of Warfare", *SC Magazine*, Sec. Content, 27 agosto, 2008, https://www.scmagazine.com/perspective/cyberspace-and-the-changing-nature-of-warfare

5 Andrew Cooper et al., "Introduction: The Challenges of 21st-Century Diplomacy" en *The Oxford Handbook of Modern Diplomacy*, eds. Andrew Cooper et al. (Oxford: Oxford University Press, 2013): 1-31.

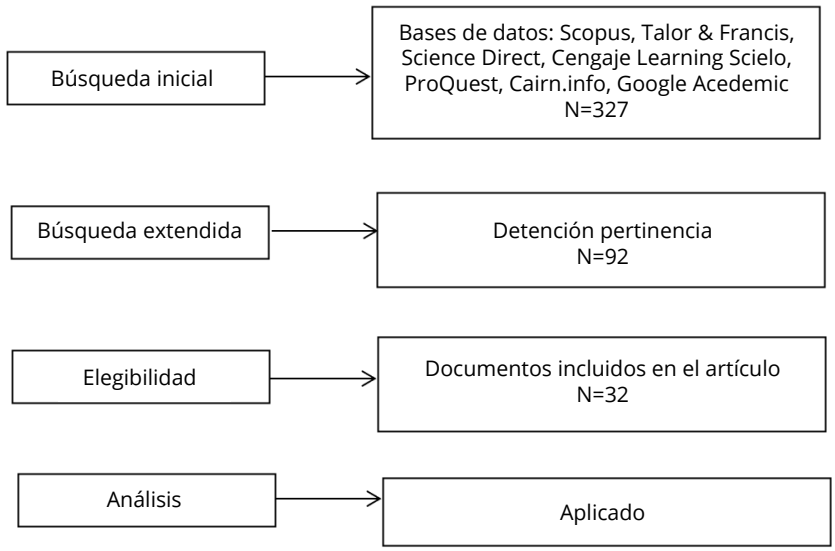
gestionar estos temas comúnmente afectantes, se ha desarrollado un nuevo ámbito diplomático: la diplomacia cibernética. En virtud de lo anterior, la pregunta de investigación que explora este artículo es: ¿en qué términos se plantea la relación entre la ciberdiplomacia y el ciberpoder de un país, para alcanzar sus intereses nacionales en tiempos modernos, a partir de la inclusión del ciberespacio como dominio de guerra por la OTAN?

El presente artículo tiene como objetivo analizar las dinámicas que acontecen en el ciberespacio y las amenazas a la estabilidad de las naciones en la puja por el poder, como exponer las acepciones de la ciberdiplomacia con sus variables constitutivas y la importancia de esta en el actual mundo globalizado. Se dará paso a un análisis descriptivo de cómo y por qué opera la ciberdiplomacia, sus elementos constitutivos y otros mecanismos que le son propios y, en consecuencia, se adscriben al ciberpoder de un Estado o una nación. Se busca de la noción de ciberdiplomacia ampliar la comprensión tanto teórica como práctica de sus procedimientos y roles en el sistema internacional contemporáneo[6].

Metodológicamente, la investigación se abordó mediante revisión sistemática, combinada con datos provenientes de múltiples análisis primarios o investigaciones individuales con las palabras de ciberdiplomacia, diplomacia cibernética y ciberpoder, posteriores a 2010. Con estas premisas se indagó en los metabuscadores DuckDuckGo y Metacrawler y en las bases de datos Scopus, Taylor & Francys, Science Direct, Cengage Learning Scielo, ProQuest, Cairn.info, Google Académico, etc. A los contenidos presentes en estas y otras fuentes documentales, se integraron las publicaciones pertenecientes a la denominada "literatura gris", la cual engloba experiencias documentadas en revistas no contempladas por motores de búsqueda de alcance general como Google Académico, para recopilar fuentes relevantes como informes de la industria, sitios web y libros. Además, se incorporó la interpretación desarrollada por la investigadora con base en la experiencia en campo y de cara a la comprensión del ciberespacio y su perspectiva crítica acerca de la ciberdiplomacia y sus prácticas.

[6] Radu Mureşan, "Current Approaches of Diplomacy in the Cyberspace", *Studia Universitatis Babes-Bolyai-Studia Sociologia* 62, núm. 2 (2017).

Figura 1. Búsqueda sistematizada



Fuente: elaboración propia.

El ciberespacio en el sistema internacional

"La esfera digital ha penetrado profundamente nuestras vidas personales y a la sociedad en su conjunto", afirma Josepha Ivanka Wessels, en un documento del Centro de Resolución de Conflictos Internacionales (CRIC) de la Universidad de Copenhague. Esta cuestión denota una observación clara y atinada: "la era digital abre nuevos terrenos para la investigación de la paz y el conflicto"[7]. Desde el momento en el que los Estados reconocieron las tecnologías de redes globales interconectadas, como instrumentos que podrían ser valiosos en la administración de sus asuntos, en la expansión de su influencia y poder en el mundo digital, ha surgido una discusión tanto entre los Estados como en el ámbito académico en relación con las posibles consecuencias económicas, políticas, sociales y legales a escala internacional, que alteran la seguridad y defensa nacional.

Aunado a esto, "el fenómeno de globalización por medio de las nuevas tecnologías y los medios de comunicación masiva ha impulsado las relaciones de forma más

[7] Josepha Wessels, "Introduction: The Digital Age Opens Up New Terrains for Peace and Conflict Research", *Conflict and Society* 3, núm. 1 (2017): 125-129, https://www.berghahnjournals.com/view/journals/conflict-and-society/3/1/arcs030110.xml

directa entre los ciudadanos y los colectivos"[8], lo que ha propiciado un acceso más inmediato a información diversa y ha facilitado la comunicación entre individuos y grupos, al superar barreras geográficas y culturales.

Puesto que en el siglo XXI se ha desarrollado el mundo de la cibercultura, en torno a lo digital, lo que la voluntad de un Estado puede pretender imponer sobre otro obedece a la más variada naturaleza. Abarca lo económico, lo político, lo cultural, los recursos naturales y los recursos humanos, por lo que estas nuevas formas de guerra podrían tener consecuencias inusitadas e imprevistas[9].

Montero, Jiménez y Ardila afirman que "la evolución del conflicto armado a lo largo de la historia de las sociedades se ha visto influenciada por una serie de variables del contexto tanto interno como externo de los intervinientes"[10]. En situaciones de conflicto o guerra, pero también en escenarios donde esta no ha sido declarada, como afirmarían Hardt y Negri[11], han venido suscitándose diferentes tipos de incidentes en el ciberespacio, ataques o conflictos que reflejan la competencia por el poder entre Estados, empresas u organismos nacionales e internacionales.

Como bien lo afirman Quiñonez, Reyes y León, "un elemento esencial en las confrontaciones que tienen lugar en el siglo XXI es el ciberespacio, pues el mundo contemporáneo demanda una geopolítica determinada por el acceso a la información y la disposición, el despliegue y el empleo de Fuerzas Militares más allá de ámbitos físicos"[12]. Valeriano y Maness[13] sostienen que, en el ciberespacio, la competencia por el poder y la influencia son elementos centrales para la ciberseguridad y el ciberconflicto. Este enfoque tiene importantes implicaciones para la política y la seguridad internacional, ya que el ciberespacio se convierte en un nuevo ámbito de competencia estratégica.

8 Jairo Vladimir Llano Franco, "Pluralismo jurídico, diversidad cultural, identidades, globalización y multiculturalismo: perspectiva desde la ciencia jurídica", *Novum Jus* 10, núm. 1 (2016), https://novumjus.ucatolica.edu.co/article/view/1176

9 Lina María Patricia Manrique Villanueva y Gladys Elena Medina Ochoa, "Ética militar y ciberseguridad", en *Ética militar y nuevas formas de guerra: retos para las Fuerzas Armadas colombianas*, eds. Jonnathan Jiménez-Reina et al. (Bogotá: Esmic, 2021).

10 Luis Alexander Montero Moncada et al., "Efectos geopolíticos de la guerra de Ucrania", *Novum Jus* 17, núm. 1 (2023), https://doi.org/10 .14718/NovumJus.2023.17 .1.9

11 Michael Hardt y Antonio Negri, *Multitud: guerra y democracia en la era del imperio* (Barcelona: Debate, 2004).

12 Ivonne Patricia León et al., "Las Fuerzas Armadas de Colombia en misiones de paz: perspectivas y oportunidades en el contexto del posacuerdo", *Novum Jus* 16, núm. 1 (2022), https://novumjus.ucatolica.edu.co/article/view/4312

13 Brandon Valeriano y Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 224.

A propósito del poder obtenido del manejo de tecnologías, información y conocimiento, la concreción de ataques contra las infraestructuras críticas cibernéticas estatales, la vulneración de la integridad y confidencialidad de datos clasificados, así como la exposición de la privacidad de información personal, dan cuenta de la necesidad de reconocer el ciberespacio, el ciberpoder y la ciberdiplomacia como elementos fundamentales en la seguridad y defensa de un Estado[14]. Así las cosas, para sobrevivir a las amenazas del sistema internacional, los Estados requieren beneficiarse del ciberespacio, porque es un elemento maleable que puede ser tratado como una herramienta[15].

La creciente importancia del ciberespacio, del ciberpoder y de la ciberdiplomacia se hace evidente a medida que los ataques cibernéticos a infraestructuras críticas y la exposición de información sensible se vuelven amenazas más significativas para la seguridad y la defensa de los Estados.

De acuerdo con el Cooperative Cyber Defence Centre of Excellence (CCDCOE), el ciberespacio fue reconocido como un instrumento de defensa colectiva, un dominio de operaciones militares "en el que la OTAN debe defenderse tan efectivamente como lo hace en el aire, en tierra y en el mar"[16]. El impacto del ciberespacio en el sistema internacional es innegable y profundo. Este entorno digital ha revolucionado la forma como los Estados interactúan y han ampliado su capacidad para proyectar poder y llevar a cabo operaciones en el ciberespacio; además, ha creado nuevas oportunidades económicas, sociales e incluso militares lo que también ha introducido desafíos de seguridad. El ciberespacio ha dado lugar a un campo emergente de la diplomacia cibernética, donde los Estados negocian y cooperan en asuntos relacionados con la ciberseguridad y la gobernanza en línea.

En resumen, el ciberespacio ha transformado la dinámica del sistema internacional, incluso en la política, la economía y la seguridad global, de maneras cada vez más significativas. En consecuencia, se ha convertido en foco de las relaciones internacionales. La mayoría de las potencias globales ha incorporado las cuestiones cibernéticas a sus políticas exteriores, al adoptar estrategias cibernéticas y

[14] Khatuna Burkadze, "Drifting Towards Digital Foreign Policy", *The Fletcher Forum of World Affairs* 45, núm. 2 (2021): 75, https://static1.squarespace.com/static/579fc2ad725e253a86230610/t/61282c9abec660241fe2a90d/1630022810823/Forum+Vol+45-2-part-8.pdf

[15] Gills Vilar Lopes, "Relações internacionais cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional" (Tesis doctoral, Universidade Federal de Pernambuco, 2016).

[16] Junta Interamericana de Defensa, *Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar, ámbito de operaciones ciberespacial* (Montreal: Autor, 2021), 22.

designar diplomáticos encargados de procurar estos objetivos estratégicos[17]. En palabras de Kissinger, el ciberespacio colonizó el espacio físico y desplazó las actividades que eran primordialmente manuales; con esto, sus efectos se extendieron a todos los ámbitos de la organización humana[18].

No obstante, ante el surgimiento y el incremento de amenazas híbridas presentes en el ciberespacio y dada la naturaleza anónima y encubierta de sus acciones, este dominio también se ha convertido en un factor que incrementa enormemente las tensiones y la desconfianza entre países, entre antagónicos y competidores, entre aliados contra rivales en el escenario global. Arocena y Esparza dirían: "[…] la delincuencia también se nutre de los cambios sociales"[19]. Por esta razón, se puede decir que la ciberdiplomacia exhibe una doble cara; por un lado, facilita la cooperación entre Estados, mientras que, por otro, posibilita que entre en operación toda suerte de fundamentos de lógica estratégica, tales como la disuasión, la intimidación, la demostración de fuerza o el engaño, salvo que ya no por medios convencionales, sino por recursos y capacidades propias del ciberespacio[20].

De la diplomacia a la ciberdiplomacia en la geopolítica contemporánea

La Paz de Westfalia, de 1648, estableció los cimientos de la diplomacia moderna —el principio de la soberanía estatal y el respeto mutuo entre los Estados—, basada en el realismo político y el equilibrio de poder entre las potencias europeas[21]. La diplomacia, desde la perspectiva del realismo, se enfoca en el comportamiento de los Estados en busca de su propio interés y seguridad en un sistema internacional anárquico, caracterizado por su pragmatismo y su enfoque en el poder y la competencia entre los actores estatales[22].

17 Barrinha y Renard, "Cyber-diplomacy", 1-16.

18 Henry Kissinger, *Orden mundial: reflexiones sobre el carácter de las naciones y el curso de la historia* (Bogotá: Penguin Random House, 2016), 343.

19 Lorena Alonso e Iñaki Esparza, "Los retos procesales de la criminalidad informática desde una perspectiva española", *Novum Jus* 11, núm 1 (2017): 41, https://doi.org/10.14718/NovumJus.2017.11.1.2

20 Eneken Tikk y Mika Kerttunen, *Parabasis: Cyber-Diplomacy in Stalemate* (Oslo: Norwegian Institute of International Affairs, 2018).

21 Henry Kissinger, *Diplomacy* (Ciudad de México: Routledge, 2014).

22 Hans Morgenthau, *Política entre las naciones: la lucha por el poder y la paz* (Buenos Aires: Grupo Editor Latinoamericano GEL, 1986).

Más adelante, en el siglo XIX, el liberalismo comenzó a influir en la diplomacia basada en la cooperación y el derecho internacional como componentes fundamentales para lograr la paz perpetua[23], por medio de instituciones internacionales que promuevan la cooperación y la resolución pacífica de conflictos. En la última parte del siglo XIX y el inicio del siglo XX, tras la Primera Guerra Mundial, la formación de la Sociedad de Naciones permitió que, desde la perspectiva liberal, se resaltara la importancia de trabajar juntos y la solución pacífica de conflictos, es decir, ganó relevancia la diplomacia en conjunto con múltiples naciones[24].

Durante la Guerra Fría, el neorrealismo añadió una dimensión estructural a la diplomacia realista. Desde esta perspectiva, los Estados se enfrentan a un entorno sistémico, en el que las restricciones estructurales, como la distribución de poder, influyen en sus acciones diplomáticas. Entonces, los Estados buscan el equilibrio de poder por la diplomacia para mantener su seguridad y evitar la dominación de otros actores[25].

Con la globalización, la diplomacia se expandió más allá de los gobiernos, e involucró actores no estatales y cuestiones transnacionales[26]. La interdependencia compleja y la descentralización del poder en un mundo gobernado por la guerra y el surgimiento de conflictos constantes: esta es la lectura que mejor describe el sistema internacional contemporáneo, donde opera en rigor la ciberdiplomacia. En esta suerte de orden global anómico se libra una guerra global permanente en la cual los actores, aun sin perseguir objetivos comunes y a pesar de sus desigualdades, se ven forzados a cooperar[27]. Allí tienen lugar las dos principales funciones de la ciberdiplomacia que se han señalado.

El ciberespacio suele considerarse un "común global", definido como un "dominio de recursos al que todas las naciones tienen acceso legal"[28]. El ciberespacio, entonces, es comparable a otros bienes comunes globales, como la altamar, el espacio aéreo y el espacio ultraterrestre. Se considera que se requiere un mínimo de reglas y regulaciones para garantizar el acceso de todos y evitar conflictos, que solo pueden resultar de negociaciones diplomáticas. Esos principios de la sociedad internacio-

23 Emanuel Kant, "La paz perpetua", *Revista de Estudios Sociales 1*, núm. 2 (1998).
24 Hans Kelsen, *Derecho y paz en las relaciones internacionales* (Ciudad de México: Coyoacán, 2012).
25 Kenneth Waltz, *Theory of International Politics* (Boston: McGraw-Hill, 1979).
26 Robert Keohane y Joseph S. Nye, *Power and Interdependence: World Politics in Transition* (Boston: Little and Brown, 1977).
27 Hardt y Negri, *Multitud: guerra y democracia*, 8.
28 Susan Buck, *The Global Commons: An Introduction* (Londres: Island Press), 6.

nal chocan con la naturaleza controvertida del ciberespacio, pues sus principales potencias promueven visiones, intereses y valores particulares[29].

Los orígenes de la ciberdiplomacia se sitúan a principios de la primera década del siglo XXI. A medida que los profesionales prestaban más atención a la dimensión de política exterior de la agenda cibernética, aparecían los primeros estudios orientados a las políticas que defendían la ciberdiplomacia[30]. De modo que la llegada de la era digital ha dado lugar a la ciberdiplomacia, que puede definirse "como la diplomacia en el ámbito cibernético o, en otras palabras, el uso de recursos diplomáticos y el desempeño de funciones diplomáticas para asegurar los intereses nacionales con respecto al ciberespacio"[31]. Esta puede verse como la última etapa, muy importante, del cambio progresivo del papel de la diplomacia en la era digital[32]. Por consiguiente, dada la alta interconexión transfronteriza en el ciberespacio, es imperativo que los enfoques de ciberseguridad evolucionen para abordar su dimensión internacional. En lugar de limitarse a estrategias de ciberdefensa o ciberguerra es crucial comenzar a desarrollar la disciplina de la ciberdiplomacia.

A diferencia de otras áreas del ámbito internacional es problemático para los Estados confiar en la disuasión mediante represalias cuando se trata del ciberespacio, debido en particular a conflictos con la atribución, aunque son posibles otras formas de disuasión[33]. Todas estas características hacen que tanto las relaciones cibernéticas internacionales como la gobernanza del ciberespacio sean extremadamente complejas y frágiles, pero al mismo tiempo hacen que la diplomacia sea aún más necesaria, en particular en lo que respecta (no en exclusiva) a la creación de un ambiente de confianza y cooperación entre las personas y organizaciones internacionales, por medio de la promoción de valores y normas compartidas[34].

29 Barrinha y Renard, "Cyber-diplomacy", 1-16.

30 Evan Potter, ed., *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Kingston: McGill-Queen's University Press, 2002), 220.

31 Barrinha y Renard, "Cyber-diplomacy", 1-16.

32 Barrinha y Renard, "Cyber-diplomacy", 1-16.

33 Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security 41*, núm. 3 (2017): 44-71; Sico van der Meer, "Enhancing International Cyber Security: A Key Role for Diplomacy", *Security and Human Rights 26* (2015): 193-205, https://www.shrmonitor.org/assets/uploads/2017/09/SHRS_026_02-04_Van-der-Meer.pdf

34 Barrinha y Renard, "Cyber-diplomacy", 1-16.

Avinash Kumar[35] afirma que la ciberdiplomacia mediante negociaciones ayuda a evitar la escalada de un conflicto y reduce las brechas entre naciones durante una ciberguerra o durante la realización de ciberataques. Define el término como una infusión de tecnología moderna y diplomacia convencional, como una herramienta adecuada para el futuro.

En la era digital, la ciberdiplomacia emergió como un nuevo campo que explora cómo las tecnologías digitales están transformando las prácticas diplomáticas y las relaciones internacionales[36]. De ahí que, con el diálogo diplomático y la negociación de acuerdos, los países pueden abordar diferencias y resolver disputas relacionadas con la ciberseguridad, la protección de datos y otros aspectos críticos del ciberespacio.

Además, al promover la transparencia y la confianza mutua, la ciberdiplomacia reduce la probabilidad de malentendidos y malas interpretaciones que podrían desencadenar conflictos no deseados. Al fomentar la colaboración, en lugar de la confrontación, la ciberdiplomacia contribuye a preservar un entorno en el que las personas y las instituciones puedan utilizar los servicios cibernéticos con la expectativa de seguridad razonable, donde se gestione pacíficamente el cambio y se resuelvan las tensiones para evitar que estas escalen hacia un conflicto cibernético.

La ciberdiplomacia es un campo emergente de estudio, y centrado en la coordinación transfronteriza entre actores soberanos para abordar cuestiones de importancia colectiva relacionadas con la digitalización de la sociedad, las tecnologías emergentes, el entorno de amenazas y otras consecuencias que surgen de estos desarrollos[37]. Por eso está surgiendo un mayor discernimiento de la ciberdiplomacia, como un campo teórico que tiene la capacidad de ofrecer una comprensión más profunda de cómo evoluciona el sistema internacional, en un contexto de creciente digitalización, y proporcionar conocimientos valiosos para utilizarlos en la práctica de la ciberdiplomacia.

Visto de esta forma, la ciberdiplomacia presenta una relación directamente proporcional con el crecimiento del ciberespacio y sus múltiples usos, orientados a atender

[35] Avinash Kumar, "Cyber Diplomacy: The Concept, Evolution and its Applicability", *International Journal of Cyber Diplomacy* 3 (2022): 23-32, http://dx.doi.org/10.54852/ijcd.v3y202203

[36] Shaun Riordan, *Cyberdiplomacy: Managing Security and Governance Online* (Londres: Polity, 2019).

[37] Carmen-Elena Cîrnu y Alexandro Georgescu, "A Complex System Governance Theory and Conceptual Links to Cyber Diplomacy", *Studies in Informatics and Control* 32, núm. 2 (2023), https://www.researchgate.net/publication/372005481_A_Complex_System_Governance_Theory_and_Conceptual_Links_to_Cyber_Diplomacy

las mencionadas cuestiones de importancia colectiva, en tanto se fundamentan en una racional lógica de cooperación; a la vez, también conserva una relación directa con los potenciales de conflicto que el uso masivo e intensivo del ciberespacio se haga para gestionar asuntos críticos de la política internacional, pues, por más que se lleven a cabo en el ciberespacio, remiten a intereses y activos concretos vitales para los Estados nación. De allí la preocupación porque este desarrollo sea asimétrico y otorgue ventaja estratégica a algunos actores, en cuyo caso, la ciberdiplomacia adquiere un carácter preventivo, de contención de un importante número de conflictos que tienen su génesis en el mismo ciberespacio[38].

En otras palabras, la ciberdiplomacia se ocupa tanto de regular las relaciones diplomáticas tradicionales[39] como de construir un nuevo modelo de diplomacia, referido estrictamente a las cuestiones que tienen vínculo directo con el entorno ciberespacial.

Contexto estratégico de la ciberdiplomacia

En la era digital, las interacciones en el ciberespacio representan desafíos multidimensionales y entrelazados entre actores estatales y no estatales, que no pueden ser comprendidos con modelos lineales o tradicionales. La ciberdiplomacia se refiere al uso de herramientas y la mentalidad diplomática para resolver problemas que surgen del ciberespacio[40]. Y opera en un espacio donde los efectos de las acciones se propagan de manera no lineal, pues las relaciones entre diferentes actores están interconectadas en formas intrincadas.

En este escenario, la ciberdiplomacia se convierte en un mecanismo crucial para abordar la interdependencia tecnológica, la seguridad digital y la cooperación transnacional, que requiere ser estudiada con una lente analítica para comprender la naturaleza interconectada de las relaciones internacionales en el entorno cibernético y la necesidad de enfoques adaptativos y flexibles[41]. Los enfoques deben ser flexibles, adaptables y capaces de abordar los múltiples aspectos entrelazados de la ciberseguridad y la cooperación digital; por eso, la diplomacia ha sufrido trasformaciones, debido al progreso tecnológico y la incorporación del ciberespacio en

[38] Amel Attatfa et al., "Cyber Diplomacy: A Systematic Literature Review", *Procedia Computer Science* 176 (2020), https://www.sciencedirect.com/science/article/pii/S1877050920318317?via%3Dihub

[39] Victor Adrian Vevera y Sorin Topor, "Digital Diplomacy as a Management Strategy of Changes in the International Environment", *Strategic Impact* 77 (2020).

[40] Riordan, *Cyberdiplomacy*, 160.

[41] Edgar Morin, *El método 6: ética* (Madrid: Cátedra, 2004).

la sociedad contemporánea, por ejemplo, en las actividades comercial, económica, política y social de los países[42].

Para definir los actores involucrados, Barrinha y Renard[43] afirman que la ciberdiplomacia puede ser implementada total o parcialmente por diplomáticos, en formatos bilaterales o foros multilaterales. Involucra múltiples partes interesadas, como es el caso de actores no estatales, líderes de empresas tecnológicas, científicos y la misma sociedad civil. No es suficiente que un actor del sistema internacional confíe únicamente en soluciones técnicas para resolver problemas de gobernanza, ciberseguridad, cibercrimen y se hace recurrir a la ciberdiplomacia para complementarlo[44].

Autores como Tiirmaa-Klaar[45], Areng[46], Carmen-Elena Cîrnu y Georgescu[47] identifican algunas áreas que requieren atención prioritaria en el ámbito de la ciberdiplomacia. Tiirmaa-Klaar define cinco: derechos humanos, seguridad global, gobernanza en línea, delitos cibernéticos y fortalecimiento de capacidades, mientras que Areng argumenta la necesidad de compartir mejores prácticas entre los gobiernos, desarrollar capacidades cibernéticas en especial con los países con menos recursos, y la realización de ejercicios a escala nacional y multinacional. Por su parte, Carmen-Elena Cîrnu y Georgescu establecen que el ciberdelito, la gobernanza, la propiedad intelectual, la protección de la privacidad, la autonomía estratégica, los estándares, la guerra cibernética, las tecnologías emergentes y la soberanía digital forman parte del dominio cibernético.

42 Danna Valentina Álvarez Guzmán, "La diplomacia en la era digital: un dialogo sobre los procesos de transformación diplomática surgidos a raíz de los avances tecnológicos", *Relaciones Internacionales*, núm. 48 (2021), https://revistas.uam.es/relacionesinternacionales/article/view/13452/14028

43 Barrinha y Renard, "Cyber-diplomacy", 1-16.

44 Riordan, *Cyberdiplomacy*, 160.

45 Heli Tiirmaa-Klaar, "Cyber Diplomacy: Agenda, Challenges and Mission", en *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallin: OTAN, 2013), 509-529.

46 Ioana-Cristina Vasiloiu, "Cyber Diplomacy: A New Frontier for Global Cooperation in the Digital Age", *Informática Económica* 27, núm. 1 (2023), https://ideas.repec.org/a/aes/infoec/v27y2023i1p41-50.html

47 Cîrnu y Georgescu, "A Complex System Governance Theory", 127-136.

Tabla 1. Áreas de interés de la ciberdiplomacia

Áreas de interés de la ciberdiplomacia	Tiirmaa-Klaar	Areng	Carmen-Elena Cîrnu y Georgescu
Derechos humanos	X		
Protección datos personales			X
Seguridad global	X		
Ejercicios cibernéticos		X	
Guerra cibernética			X
Mejores prácticas entre los gobiernos		X	
Estándares			X
Gobernanza digital	X		X
Ciberdelito	X		X
Fortalecimiento de capacidades	X	X	
Propiedad intelectual			X
Tecnologías emergentes			X
Soberanía digital			X

Fuente: elaboración propia.

Desde la mirada interpretativa y comprehensiva de la investigadora en temas asociados con el ciberespacio y con base en los estudios realizados, se proponen cinco particularidades clave como categorías de análisis para estudiar la ciberdiplomacia desde la perspectiva de la cooperación. Estas corresponden a las áreas de interés de la ciberdiplomacia que son comunes a los autores sintetizados en la Tabla 1, en contraste con las necesidades mostradas con suma claridad por las nuevas dinámicas tecnológicas, así:

a. Seguridad global: la diplomacia cibernética cumple una función indispensable en la mitigación de conflictos, en el fomento de la estabilidad y la protección de los intereses nacionales y los derechos humanos en un contexto global caracterizado por una creciente interconexión. En el siglo XXI, las amenazas no se circunscriben al plano físico, sino que hacen uso del dominio virtual llamado ciberespacio, el cual emergió como un nuevo escenario donde actores estatales y no estatales pueden llevar a cabo acciones que fortalezcan la seguridad de naciones, instituciones, empresas y sociedad civil, centrados en la prevención de conflictos en el ciberespacio y la protección de infraestructuras críticas nacionales.

b. Gobernanza cibernética: la ciberdiplomacia y la gobernanza cibernética presentan una estrecha relación, toda vez que se ocupan de asuntos internacionales

en el ciberespacio. Mientras la primera se enfoca en las relaciones bilaterales y multilaterales y otros actores en el mundo digital, la segunda se centra en el desarrollo de políticas y normas globales; por ende, la colaboración y la cooperación internacionales son fundamentales para garantizar un entorno en línea que proteja los intereses de todos los actores y promueva la seguridad y la estabilidad en el ciberespacio.

c. Cibercrimen: la ciberdiplomacia permite la colaboración global, componente esencial para abordar la creciente amenaza del cibercrimen y proteger los intereses de la comunidad internacional en el ciberespacio. Además, aporta significativamente a la lucha contra el cibercrimen por medio de la cooperación internacional, del establecimiento de normas y tratados, de la prevención de conflictos cibernéticos y de la promoción de la ciberseguridad. Permite suscribir acuerdos o alianzas internacionales para rastrear y perseguir a cibercriminales trasfronterizos, debido a la naturaleza transnacional del cibercrimen.

d. Fortalecimiento de capacidades cibernéticas: la ciberdiplomacia y el fortalecimiento de capacidades cibernéticas se complementan en varios aspectos, como la colaboración internacional en temas asociados con la promoción de estándares y normas, la cooperación en respuesta a incidentes para investigar y dar respuesta efectiva, la negociación de acuerdos bilaterales y multilaterales para contribuir al desarrollo de capacidades de otros países y la prevención de conflictos en el ciberespacio, y la promoción de un entorno digital seguro.

e. Soberanía digital: la ciberdiplomacia desempeña un papel fundamental en el fomento de la soberanía digital. Permite a los países colaborar en el desarrollo de normas y principios que respeten la soberanía digital de cada uno, al mismo tiempo que abordan desafíos transnacionales. Al buscar acuerdos internacionales y participar en diálogos diplomáticos en el ámbito cibernético, los Estados pueden trabajar juntos para proteger su capacidad de tomar decisiones autónomas sobre asuntos relacionados con el ciberespacio. Esto implica la defensa de la capacidad de un país para gestionar y regular sus propias infraestructuras digitales, proteger la privacidad de sus ciudadanos y garantizar la integridad de sus datos en línea. La ciberdiplomacia permite a los países colaborar en el desarrollo de normas y principios que respeten la soberanía digital de cada uno, mientras se abordan desafíos transnacionales como la ciberseguridad, la ciberdefensa, la ciberresiliencia, la ciberdelincuencia y el ciberpoder.

En tanto la ciberdiplomacia podría ser un elemento constitutivo del poder nacional en general y del ciberpoder en particular, exhibe su naturaleza o vínculo con el potencial bélico, justamente porque determinado uso del ciberespacio bien puede constituirse como herramienta, estrategia o, digámoslo sin ambages, en un arma.

Ciberdiplomacia en relación con el ciberpoder

Hoy en día, la tecnología está progresando a ritmos exponenciales y un ejemplo de esto es que el tejido de la vida humana se entrelaza con el ciberespacio. Allí, donde cada conexión encuentra su eco en esta vasta red digital, almacenada quizás en bases de datos que abarcan desde información de carácter personal hasta cuestiones políticas, económicas y sociales, incluso militares o de seguridad nacional. A raíz de estos eventos recientes y su evolución es esencial comprender la vastedad del concepto de ciberpoder, ya que engloba diversos elementos que afectan el comportamiento y la influencia de las naciones, al trascender las fronteras tradicionales basadas en la geografía terrestre, marítima o aérea[48].

Victor Luke[49] sostiene que en la actualidad se viven épocas de cambios de poder. Las fronteras son líneas digitales, presentes en el ciberespacio. Hay una nueva forma de ver la geopolítica en un mundo marcado por las tecnologías de información y las tecnologías de operación. Norberto Bobbio define el poder como la "capacidad de una persona de influir, condicionar y determinar el comportamiento de otro individuo"[50]. Este fenómeno sugiere que el poder implica la aptitud para ejercer dominio, influencia o autoridad sobre individuos o entidades. Esta influencia puede adoptar diversas manifestaciones, tales como la persuasión, la autoridad, la coerción o la capacidad para tomar decisiones que repercutan en terceros. Joseph Nye, un experto en relaciones internacionales, clasifica el poder en dos categorías: hard power y soft power. La primera se refiere al empleo de fuerzas militares para alcanzar objetivos, mientras que la segunda se caracteriza por influir en las acciones o intereses de otros actores por medios culturales, ideológicos y diplomáticos[51]. La combinación de ambas culmina en lo que se conoce como smart power o poder

[48] Jill Rowland et al., "The Anatomy of a Cyber Power", *International Journal of Critical Infrastructure Protection* 7, núm. 1 (2014), https://www.sciencedirect.com/science/article/abs/pii/S187454821400002X?via%3Dihub

[49] Victor Luke, "Seguridad informática y derecho internacional público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas", *Revista de Derecho Público*, núm. 77 (2012), https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/30935/32662

[50] Norberto Bobbio, "El estado de naturaleza, la sociedad civil y el estado racional", *Revista Mexicana de Ciencias Políticas y Sociales 28*, núm. 110 (1982): 135.

[51] Joseph S. Nye, *Bound to Lead: The Changing Nature of American Power* (Nueva York: Basic Books, 1990), 307.

inteligente, el cual es definido por Armitage y Nye como "una aproximación que destaca la necesidad de una armada fuerte y organizada, así como también el establecimiento de todo tipo de alianzas y de asociaciones, tanto entre países como entre instituciones, y a todos los niveles"[52]. Con el poder inteligente, se puede precisar la habilidad para gestionar y supervisar el ciberespacio. De esta manera, el ejercicio del poder sobre el ciberespacio implica la evaluación y la definición del uso de la información, con el fin de establecer dominio en dicho ámbito.

Para comprender mejor las acciones de los Estados y el poder nacional en la actualidad es útil conceptualizar el poder cibernético, compuesto de objetivos que los Estados intentarán alcanzar desde el ciberespacio. Hoy, los países no solo buscan destruir y deshabilitar la infraestructura y las capacidades del adversario, pues se busca fortalecer y mejorar las defensas cibernéticas nacionales, reunir inteligencia en otros países, hacer crecer la industria cibernética nacional, competir, controlar y manipular el entorno de la información, y extender la influencia mediante normas y estándares internacionales y estándares técnicos[53]. En este escenario, la ciberdiplomacia, como parte de la diplomacia científica, representa un factor esencial para fortalecer el ciberpoder de una nación.

Para clarificar la relación entre ciberdiplomacia y ciberpoder conviene llevar a cabo una breve formulación y un análisis estructurado del lugar que ocupa cada concepto en el marco de los asuntos estratégicos de los Estados. La ciberdiplomacia se adelanta con mecanismos y procedimientos; entre tanto, el ciberpoder se ejerce mediante estrategias, muchas de ellas, militares.

En primer lugar, si bien la ciberdiplomacia es una práctica distintiva reciente, de suma relevancia para las relaciones internacionales en el contexto contemporáneo, no necesariamente es un elemento constitutivo del ciberpoder. Es más acertado afirmar que es una herramienta, una serie de procedimientos protocolizados que potencia por otra vía, la obtención de los intereses nacionales[54].

Ahora bien, que este mecanismo resulte útil para hacer uso efectivo del ciberpoder, es otra cuestión que se ubica en los límites de las regulaciones del derecho

[52] Richard Lee Armitage y Joseph S. Nye, *CSIS Commission on Smart Power: A Smarter, more Secure America* (Washington: CSIS, 2007), 7.

[53] Julia Voo et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations* (Cambridge: Harvard Kennedy School, 2020), 84.

[54] Pierre Pahlavi, "Cyber-diplomacy: A New Strategy of Influence", *Canadian Political Association General Meeting* 30 (2003): 1-27.

internacional humanitario y la esfera ética, que juzga las acciones en circunstancias de conflicto. Se estaría remitiendo al uso de estratagemas como la confusión y el engaño, de no extraña ocurrencia en la diplomacia tradicional, mediante formas que se sirven de la tecnología para fines idénticos. Quizás se cuenta con mayores recursos para lograrlo, si se piensa en la dilación de negociaciones o la manifestación de apoyo a determinado acuerdo o tratado, mientras se provocan ataques masivos para presionar a la opinión pública y la agenda política[55], con la particular "ventaja" de que exista una alta probabilidad de que la autoría de esta suerte de "juego sucio" nunca sea develada. Esto en verdad transforma las relaciones internacionales y deja ver el aspecto paradigmático y controvertido tanto de la ciberdiplomacia como del ciberpoder, puesto que, a efectos del caso hipotético que se ha presentado, difícilmente el infractor podrá ser imputado con cargos por perfidia o delito similar.

Respecto a los mecanismos, los procedimientos mediante los cuales opera la ciberdiplomacia, se pueden enmarcar en dos tendencias concretas: la ciberdiplomacia basada en la cooperación como fundamento de lógica estratégica, que exhibe connotaciones positivas, incluso altruistas[56] tiene como propósito primordial fortalecer la colaboración internacional, con el fin de abordar los obstáculos y retos propios del ciberespacio y garantizar la seguridad y la estabilidad del entorno digital global. Para ello, los actores en el ciberespacio —gobiernos, organizaciones, corporaciones, sector privado y sociedad civil— deben colaborar, negociar y desarrollar capacidades cibernéticas independientes, pero también, en alguna medida, afines.

De allí que sea adecuado aproximarse a este enfoque de la ciberdiplomacia desde los ejes de análisis identificados en este escrito: seguridad global, gobernanza cibernética, cibercrimen, fortalecimiento de capacidades cibernéticas y soberanía digital. Nótese que, en cualquier caso, se trata de temas de interés global, en los cuales participar conlleva siempre mayores beneficios que riesgos. Desde esta perspectiva, la ciberdiplomacia es un vehículo cada vez más instituido, consolidado y formalizado en el marco de las instancias reguladoras del Sistema Internacional contemporáneo.

La segunda tendencia corresponde a la ciberdiplomacia como parte del arsenal que constituye el poder de combate de un país, concretamente de la fracción de este que corresponde al ciberpoder. Allí operan otras lógicas y otros fundamentos, como la

[55] Mureşan, "Current Approaches of Diplomacy in the Cyberspace", 31-43.

[56] Jorge M. Vega, "Ciberdiplomacia en América Latina: niveles, enfoques y velocidades", *Análisis del Real Instituto Elcano*, núm. 38 (2023): 7, https://media.realinstitutoelcano.org/wp-content/uploads/2023/05/ari38-2023-vega-ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades.pdf

noción de poder, vista como la capacidad de ejercer control, influencia o autoridad sobre alguien o algo por medio de la persuasión, la autoridad, la coerción, la intimidación, el engaño o la capacidad de tomar decisiones que afecten a otros. Casi todas ellas, acciones ubicadas en el límite de las normas positivas éticas y legales[57].

Al respecto, a juicio de la investigadora y al retomar la noción de smart power (poder inteligente), este se presenta como dogma capaz de salvar las objeciones ya señaladas, al integrar y hacer uso de las ventajas peculiares de la ciberdiplomacia como su capacidad de participar y formar alianzas (soft power), sin renunciar a la posibilidad de aumentar y consolidar el ciberpoder de un país tanto como sea posible (hard power). Con ello se reafirma la premisa realista de que una gran mayoría de los países persiguen con ambición mayores capacidades en el dominio de la información y del ciberespacio, buscan aumentar su arsenal para ganar la iniciativa o retener su ventaja estratégica.

Como ya se mencionó, la ciberdiplomacia es una herramienta que permite abordar los desafíos y las oportunidades que plantea el ciberespacio en el contexto de las relaciones internacionales, con el propósito de establecer un marco de cooperación y respeto mutuo entre los Estados en el ámbito digital.

Por su parte, el ciberpoder puede permitir a los actores alcanzar una serie de objetivos en el ciberespacio, que van desde la seguridad y la defensa hasta la influencia geopolítica y la prosperidad económica. Sin embargo, también conlleva responsabilidades y desafíos, como la necesidad de actuar de manera responsable y respetar las normas internacionales; por ello queda sentada la estrecha relación de interdependencia entre la ciberdiplomacia y el ciberpoder de una nación.

Conclusiones

En el presente trabajo se planteó como objetivo alcanzar claridad tanto teórica como práctica del concepto de ciberdiplomacia en relación con el ciberpoder de los países, en aras de comprender las circunstancias y la manera cómo opera la ciberdiplomacia en la época contemporánea, dada la importancia vital del ciberespacio como dominio de la guerra. La formulación misma del título que designa este trabajo ya implica determinada atribución de roles a cada concepto, a saber:

[57] Daniel Dumitru y Cristina Bodoni, "Extension of International Humanitarian Law Order in the Information Area Through Digital Diplomacy", *Strategic Impact* 80, núm. 3 (2021): 17, https://revista.unap.ro/index.php/Impact_en/article/view/1341/1301

la ciberdiplomacia es y funciona con mecanismos y procedimientos, en tanto el ciberpoder lo hace por medio de estrategias. El propósito común que persigue es el logro de los intereses nacionales. Así, todos los argumentos dispuestos y ofrecidos giraron en torno a delimitar esta relación en primera instancia y a describir los denominados mecanismos con los cuales la ciberdiplomacia produce sus efectos, tanto en el ámbito físico como en el entorno digital.

La gran conclusión es que la mayor fortaleza de la ciberdiplomacia no es permitir la cooperación, beneficiar con medios tecnológicos los buenos oficios diplomáticos de los países, aumentar la oportunidad, la agilidad y la obtención de resultados bilaterales o multilaterales; más allá, en la práctica, sus mecanismos favorecen la integración de sus procedimientos a diversas estrategias y planes de acción que diseñan los países para preservar la seguridad y defensa de sus intereses.

Las categorías y relaciones que se definieron entre ciberpoder, ciberdiplomacia, mecanismos y estrategias dejaron claro que el smart power estaba en el centro de las cuestiones relativas a la integración y maximización de capacidades cibernéticas adscritas al poder nacional de los países. En la búsqueda de aquellos mecanismos queda por responder ¿cómo opera la ciberdiplomacia en el escenario estratégico global? Se trata de la teoría de la gobernanza en sistemas complejos y su relación con la ciberdiplomacia[58], aproximación conceptual que reviste para este trabajo académico el mayor interés.

En pleno acuerdo con lo que ha sido documentado en este escrito, la ciberdiplomacia es un campo de estudio emergente, que se enfoca en las coordinaciones entre actores más allá de sus fronteras, para resolver asuntos de importancia colectiva relacionados con la digitalización de la sociedad, las tecnologías emergentes, el surgimiento de nuevas amenazas y las consecuencias no previstas del desarrollo de este entorno.

Desde este punto de partida, la autora analiza la ciberdiplomacia a la luz de la teoría de la gobernanza de sistemas complejos, con base en la premisa de que, en efecto, el sistema internacional contemporáneo es consistente con la descripción de un sistema complejo; por ello es susceptible de ser estudiado desde la descripción de sistema de sistemas. La ciberdiplomacia puede ser integrada a su vez en esta perspectiva, tras la observación y el análisis de la integración de actores por medio de la comunicación y la coordinación.

[58] Cîrnu y Georgescu, "A Complex System Governance Theory", 127-136.

Este trabajo comporta una aproximación inédita a las investigaciones futuras, referentes a la ciberdiplomacia e incluye métodos como el modelamiento y la simulación. No obstante, hay que anotarlo, se queda corta en su alcance, puesto que, al desligar por completo la ciberdiplomacia del ciberpoder, se torna en un trabajo que aporta a los mecanismos y procedimientos que regulan la cooperación, pero dice poco sobre las otras dinámicas que hemos estudiado, aquellas que se localizan en el centro de los ciberconflictos. En consecuencia aporta marginalmente a la reflexión y configuración práctica de los sistemas de ciberdefensa de los países, en los cuales radica la consecución y la retención de los siempre valorados intereses nacionales.

Referencias

Alonso, Lorena e Iñaki Esparza. "Los retos procesales de la criminalidad informática desde una perspectiva española". *Novum Jus* 11, núm 1 (2017): 39-72. https://doi.org/10.14718/NovumJus.2017.11.1.2

Álvarez Guzmán, Danna Valentina. "La diplomacia en la era digital: un dialogo sobre los procesos de transformación diplomática surgidos a raíz de los avances tecnológicos". *Relaciones Internacionales*, núm. 48 (2021): 285-292. https://revistas.uam.es/relacionesinternacionales/article/view/13452/14028

Armitage, Richard Lee y Joseph Nye. *CSIS Commission on Smart Power: A Smarter, more Secure America*. Washington: CSIS, 2007.

Attatfa, Amel, Karen Renaud y Stefano de Paoli. "Cyber Diplomacy: A Systematic Literature Review". *Procedia Computer Science* 176 (2020): 60-69. https://www.sciencedirect.com/science/article/pii/S1877050920318317?via%3Dihub

Barrinha, André y Thomas Renard. "Cyber-diplomacy: The Making of an International Society in the Digital Age". *Global Affairs* (2017): 1-16. https://doi.org/10.1080/23340460.2017.1414924

Bobbio, Norberto. "El estado de naturaleza, la sociedad civil y el estado racional". *Revista Mexicana de Ciencias Políticas y Sociales* 28, núm. 110 (1982): 135.

Buck, Susan. *The Global Commons: An Introduction*. Londres: Island Press, 1998.

Burkadze, Khatuna. "Drifting Towards Digital Foreign Policy". *The Fletcher Forum of World Affairs* 45, núm. 2 (2021): 75-88. https://static1.squarespace.com/static/579fc2ad725e253a86230610/t/61282c9abec660241fe2a90d/1630022810823/Forum+Vol+45-2-part-8.pdf

Cîrnu, Carmen-Elena & y Alexandro Georgescu. "A Complex System Governance Theory and Conceptual Links to Cyber Diplomacy". *Studies in Informatics and Control* 32, núm. 2 (2023): 127-136. https://www.researchgate.net/publication/372005481_A_Complex_System_Governance_Theory_and_Conceptual_Links_to_Cyber_Diplomacy

Cooper, Andrew, Jorge Heine y Ramesh Thakur. "Introduction: The Challenges of 21st-Century Diplomacy" en *The Oxford Handbook of Modern Diplomacy*, editado por Andrew Cooper, Jorge Heine y Ramesh Thakur, 1-23. Oxford: Oxford University Press, 2013.

Dumitru, Daniel y Cristina Bodoni. "Extension of International Humanitarian Law Order in the Information Area Through Digital Diplomacy". *Strategic Impact* 80, núm. 3 (2021): 86-102. https://revista.unap.ro/index.php/Impact_en/article/view/1341/1301

Eriksson, Johan y Giampiero Giacomello. "Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty" en *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, editado por Myriam Dunn Cavelty y Andreas Wenger, 95-107. Nueva York: Routledge, 2022.

Geers, Kenneth. "Cyberspace and the Changing Nature of Warfare". *SC Magazine*, Sec. Content, 27 agosto, 2008. https://www.scmagazine.com/perspective/cyberspace-and-the-changing-nature-of-warfare

Hardt, Michael y Antonio Negri. *Multitud: guerra y democracia en la era del imperio*. Barcelona: Debate, 2004.

Junta Interamericana de Defensa. *Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar, ámbito de operaciones ciberespacial*. Montreal: Autor, 2021.

Kant, Emanuel. "La paz perpetua". *Revista de Estudios Sociales* 1, núm. 2 (1998): 142-144.

Kelsen, Hans. *Derecho y paz en las relaciones internacionales*. Ciudad de México: Coyoacán, 2012.

Keohane, Robert O. y Joseph S. y Nye. *Power and Interdependence: World Politics in Transition*. Boston: Little and Brown, 1977.

Kissinger, Henry. *Diplomacy*. Ciudad de México: Routledge, 2014.

Kissinger, Henry. *Orden mundial: reflexiones sobre el carácter de las naciones y el curso de la historia*. Bogotá: Penguin Random House, 2016.

Kumar, Avinash. "Cyber Diplomacy: The Concept, Evolution and its Applicability". *International Journal of Cyber Diplomacy* 3 (2022): 23-32. http://dx.doi.org/10.54852/ijcd.v3y202203

León, Ivonne Patricia, Julio Quiñónez Páez y Pablo Ignacio Reyes Beltrán. "Las Fuerzas Armadas de Colombia en misiones de paz: perspectivas y oportunidades en el contexto del posacuerdo". *Novum Jus* 16, núm. 1 (2022): 133-166. https://novumjus.ucatolica.edu.co/article/view/4312

Llano Franco, Jairo Vladimir. "Pluralismo jurídico, diversidad cultural, identidades, globalización y multiculturalismo: perspectiva desde la ciencia jurídica". *Novum Jus* 10, núm. 1 (2016): 49-92. https://novumjus.ucatolica.edu.co/article/view/1176

Lopes, Gills Vilar. "Relações internacionais cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional". Tesis Doctoral, Universidade Federal de Pernambuco, 2016.

Luke, Victor. "Seguridad informática y derecho internacional público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas". Revista de Derecho Público, núm. 77 (2012): 405-424. https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/30935/32662

Manrique Villanueva, Lina María Patricia y Gladys Elena Medina Ochoa. "Ética militar y ciberseguridad", en *Ética militar y nuevas formas de guerra: retos para las Fuerzas Armadas colombianas*, editado por Jonnathan Jiménez-Reina, Erika Constanza Figueroa-Pedreros y Martin Bricknell, 153-176. Bogotá: Esmic, 2021.

Montero Moncada, Luis Alexander, Jonnathan Jiménez Reina y Carlos Alberto Ardila Castro. "Efectos geopolíticos de la guerra de Ucrania". *Novum Jus* 17, núm. 1 (2023): 205-235. https://doi.org/10 .14718/NovumJus.2023.17 .1.9

Morgenthau, Hans. *Política entre las naciones: la lucha por el poder y la paz*. Buenos Aires: Grupo Editor Latinoamericano GEL, 1986.

Morin, Edgar. *El método 6: ética*. Madrid: Cátedra, 2004.

Mureşan, Radu. "Current Approaches of Diplomacy in the Cyberspace". *Studia Universitatis Babes-Bolyai-Studia Sociologia* 62, núm. 2 (2017): 31-43.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace". *International Security* 41, núm. 3 (2017): 44-71.

Nye, Joseph S. *Bound to Lead: The Changing Nature of American Power*. Nueva York: Basic Books, 1990.

Pahlavi, Pierre. "Cyber-diplomacy: A New Strategy of Influence". *Canadian Political Association General Meeting 30* (2003): 1-27.

Potter, Evan, ed. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. Kingston: McGill-Queen's University Press, 2002.

Riordan, Shaun. *Cyberdiplomacy: Managing Security and Governance Online*. Londres: Polity, 2019.

Rowland, Jill, Mason Rice y Sujeet Shenoi. "The Anatomy of a Cyber Power". *International Journal of Critical Infrastructure Protection* 7, núm. 1 (2014): 3-11. https://www.sciencedirect.com/science/article/abs/pii/S187454821400002X?via%3Dihub

Tiirmaa-Klaar, Heli. "Cyber Diplomacy: Agenda, Challenges and Mission" en *Peacetime Regime for State Activities in Cyberspace*, editado por Katharina Ziolkowski, 509-532. Tallin: OTAN, 2013.

Tikk, Eneken y Mika Kerttunen. *Parabasis: Cyber-Diplomacy in Stalemate*. Oslo: Norwegian Institute of International Affairs, 2018.

Valeriano, Brandon y Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press, 2015.

Van der Meer, Sico. "Enhancing International Cyber Security: A Key Role for Diplomacy". *Security and Human Rights* 26 (2015): 193-205. https://www.shrmonitor.org/assets/uploads/2017/09/SHRS_026_02-04_Van-der-Meer.pdf

Vasiloiu, Ioana-Cristina. "Cyber Diplomacy: A New Frontier for Global Cooperation in the Digital Age". *Informática Económica* 27, núm. 1 (2023): 41-50. https://ideas.repec.org/a/aes/infoec/v27y2023i1p41-50.html

Vega, Jorge M. "Ciberdiplomacia en América Latina: niveles, enfoques y velocidades". *Análisis del Real Instituto Elcano*, núm. 38 (2023): 1-7. https://media.realinstitutoelcano.org/wp-content/uploads/2023/05/ari38-2023-vega-ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades.pdf

Vevera, Victor Adrian y Sorin Topor. "Digital Diplomacy as a Management Strategy of Changes in the International Environment". *Strategic Impact* 77 (2020): 126-136.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy y Anina Schwarzenbach. *National Cyber Power Index 2020: Methodology and Analytical Considerations*. Cambridge: Hardvard Kennedy School, 2020.

Waltz, Kenneth. *Theory of International Politics*. Boston: McGraw-Hill, 1979.

Wessels, Josepha. "Introduction: The Digital Age Opens Up New Terrains for Peace and Conflict Research". *Conflict and Society* 3, núm. 1 (2017): 125-129. https://www.berghahnjournals.com/view/journals/conflict-and-society/3/1/arcs030110.xml

Wu, Jiangxing. "Cyberspace Endogenous Safety and Security". *Engineering* 15 (2022): 179-185. https://www.sciencedirect.com/science/article/pii/S2095809921003179