Geopolítica del Ciberespacio y Seguridad Nacional - Implicaciones para la Defensa de Colombia

Mayor (EJC) Harold Franco Vásquez

Artículo para optar al título profesional:

Magister en Estrategia y Geopolítica

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

DATOS GENERALES		
Nombre del estudiante	**:**	Harold Franco Vásquez
Identificación	**:**	72286189
Programa académico	**:**	Maestría Estrategia y Geopolítica
Tutor metodológico	**:**	Juan Carlos Aristizábal Murillo
Tutor temático	**:**	Mg. Julián Enrique Barrero García
Fecha de entrega	**:**	Septiembre 2025
Extensión	**:**	10310 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este artículo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Geopolítica del Ciberespacio y Seguridad Nacional - Implicaciones para la Defensa de Colombia

Sociopolitical characterization of borders in Colombia and Latin América

Harold Franco Vásquez[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El artículo analiza las implicaciones geopolíticas del ciberespacio para la seguridad y defensa nacional de Colombia. Examina tres objetivos principales: las dinámicas de poder entre Estados en el ciberespacio; las amenazas y vulnerabilidades que enfrenta el país, especialmente en su infraestructura crítica y operaciones militares; y las estrategias y políticas nacionales, con énfasis en el rol de las Fuerzas Militares y la cooperación internacional. Se empleó una metodología cualitativa basada en revisión sistemática de literatura académica y fuentes oficiales. Las conclusiones destacan que el ciberespacio es un dominio estratégico fundamental. Colombia debe fortalecer su resiliencia digital, consolidar sus capacidades defensivas y profundizar su articulación con aliados internacionales para proteger su soberanía y garantizar su estabilidad frente a amenazas cibernéticas.

Palabras clave: Ciberseguridad, geopolítica del ciberespacio, defensa nacional, Colombia, ciberdefensa, amenazas cibernéticas, soberanía digital.

Abstract: This article examines the geopolitical implications of cyberspace for Colombia's national security and defense. It addresses three main objectives: analyzing power dynamics between States in cyberspace; identifying threats and vulnerabilities to Colombia's critical infrastructure and military operations; and evaluating national strategies and policies, with emphasis on the role of the Armed Forces and international cooperation. A qualitative methodology was applied, based on a systematic review of academic literature and official sources. The findings confirm that cyberspace is a strategic domain that demands urgent attention. Colombia must enhance its digital resilience, strengthen its cyber defense capabilities, and deepen collaboration with international partners to safeguard its digital sovereignty and ensure national stability in the face of growing cyber threats.

Keywords: Cybersecurity, cyberspace geopolitics, national defense, Colombia, cyber defense, digital sovereignty, cyber threats.

[1] Mayor del Ejército Nacional de Colombia. Candidato a Magíster en estrategia y geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. - Contacto: Harold.franco@esdeg.edu.co

[T1] Introducción

El presente estudio explora la compleja relación entre la geopolítica del ciberespacio y sus profundas implicaciones para la seguridad y defensa nacional de Colombia. En un contexto global donde el ciberespacio se ha consolidado como un dominio crucial para las interacciones entre Estados y la competencia por el poder, resulta imperativo examinar cómo estas dinámicas influyen en la estrategia de defensa de la nación colombiana. Este análisis se vuelve aún más relevante en un mundo caracterizado por la creciente digitalización de la sociedad, la economía y el gobierno, donde las vulnerabilidades y las amenazas en el ciberespacio pueden tener consecuencias trascendentales para la estabilidad y el desarrollo de un país.

Para abordar esta cuestión central, la investigación se enfoca en analizar las dinámicas de poder y competencia que caracterizan las relaciones entre los Estados en el ciberespacio. Se exploran las diversas manifestaciones de estas dinámicas, desde las operaciones de influencia y el ciberespionaje hasta el desarrollo de capacidades ofensivas, con el fin de comprender su alcance y significado para la seguridad nacional. Se examina cómo los Estados utilizan el ciberespacio como una herramienta para proyectar su poder, asegurar sus intereses y competir por la influencia a nivel global. Este análisis incluye la consideración de las implicaciones éticas y legales del uso de las capacidades cibernéticas, así como los desafíos que plantea la atribución de los ataques y la regulación de la conducta de los Estados en el ciberespacio.

Asimismo, se lleva a cabo una identificación exhaustiva de las principales amenazas y oportunidades que el ciberespacio presenta para Colombia en el ámbito de la defensa. Este análisis incluye una evaluación de los riesgos asociados a los ciberataques contra la infraestructura crítica, los sistemas de información del gobierno y las operaciones militares, que son esenciales para el funcionamiento del Estado y la protección de la soberanía nacional. También se exploran las oportunidades que ofrece el ciberespacio para fortalecer las capacidades de ciberdefensa del país, como el uso de la inteligencia cibernética para la detección de amenazas, el desarrollo de sistemas de alerta temprana y la implementación de estrategias de resiliencia cibernética.

La metodología empleada en este estudio se basa en una revisión sistemática de la literatura académica y especializada. A través del análisis y síntesis de fuentes relevantes, se busca construir un marco teórico sólido que permita comprender la complejidad del fenómeno estudiado y proporcionar una base para futuras investigaciones. Este enfoque metodológico cualitativo facilita

una exploración profunda de las dinámicas en juego y contribuye a la generación de conocimiento relevante para la formulación de políticas y estrategias de ciberseguridad y defensa en Colombia. Se reconoce la importancia de considerar tanto las perspectivas teóricas como las empíricas para obtener una comprensión integral del tema y se busca integrar los hallazgos de la literatura con el contexto específico de Colombia.

Además de analizar las dinámicas de poder y competencia entre Estados, la investigación también aborda el papel de los actores no estatales en el ciberespacio, como los grupos criminales, los activistas y las organizaciones terroristas, cuyas actividades pueden tener un impacto significativo en la seguridad nacional. Se examina cómo estos actores utilizan el ciberespacio para llevar a cabo actividades ilícitas, difundir propaganda, reclutar miembros y coordinar ataques, y se exploran las estrategias que Colombia puede implementar para contrarrestar estas amenazas.

En última instancia, este estudio busca contribuir al debate académico y a la formulación de políticas sobre la geopolítica del ciberespacio y su impacto en la seguridad y defensa nacional de Colombia. Se espera que los hallazgos de la investigación proporcionen información valiosa para los responsables de la toma de decisiones, los profesionales de la seguridad y defensa, y la sociedad en general, con el fin de promover un uso seguro y responsable del ciberespacio y fortalecer la capacidad de Colombia para proteger sus intereses en este dominio crucial.

[T1] Metodología

La presente investigación adopta un enfoque metodológico cualitativo, basado en la revisión sistemática y el análisis crítico de la literatura existente sobre la geopolítica del ciberespacio y sus implicaciones para la seguridad y defensa nacional de Colombia. Siguiendo los principios de la investigación cualitativa, se busca una comprensión profunda del fenómeno estudiado, explorando las diversas perspectivas teóricas y empíricas que contribuyen a su configuración (Hernández et al, 2014). En este sentido, la revisión bibliográfica no se limita a una mera recopilación de fuentes, sino que se concibe como un proceso activo de selección, evaluación y síntesis de la información, orientado a la construcción de un marco teórico sólido y relevante para el contexto colombiano.

El proceso de revisión se estructuró en varias etapas interrelacionadas. Inicialmente, se llevó a cabo una exhaustiva búsqueda de literatura en bases de datos académicas (JSTOR, Scopus, Web

of Science, etc.) y repositorios especializados, utilizando una combinación de términos clave y operadores booleanos para identificar las fuentes más pertinentes. Se priorizó la inclusión de artículos científicos, libros, informes técnicos y documentos oficiales que abordaran directamente la temática de la investigación, considerando tanto su calidad metodológica como su actualidad y relevancia para el contexto colombiano.

La evaluación de la calidad de las fuentes se realizó mediante la aplicación de criterios explícitos, que incluyeron la rigurosidad del diseño de investigación, la validez y confiabilidad de los resultados, la claridad y coherencia de los argumentos, y la relevancia de las conclusiones para los objetivos del estudio. Se prestó especial atención a la identificación de posibles sesgos o limitaciones en las fuentes, así como a la consideración de la diversidad de perspectivas y enfoques teóricos.

El análisis de la información se llevó a cabo mediante una combinación de técnicas de análisis de contenido y análisis temático (Krippendorff, 2018). El análisis de contenido se utilizó para cuantificar la frecuencia de ciertos conceptos o temas en la literatura, mientras que el análisis temático se centró en la identificación y descripción de los patrones y relaciones entre los diferentes elementos del fenómeno estudiado. Este proceso analítico permitió sintetizar la información de manera sistemática y rigurosa, identificando las principales convergencias y divergencias en la literatura, así como los vacíos o áreas de controversia que requieren mayor investigación.

Finalmente, la investigación culminó con la elaboración de una discusión crítica de los hallazgos, en la que se contrastaron los resultados del análisis con el marco teórico de referencia y se exploraron sus implicaciones para la formulación de políticas y estrategias de ciberseguridad y defensa en Colombia. Se buscó, en todo momento, mantener una postura reflexiva y crítica frente a la literatura, reconociendo la complejidad y la multidimensionalidad del fenómeno estudiado, así como la necesidad de futuras investigaciones que profundicen en sus diversas aristas.

[T1] Desarrollo del objetivo 1

Examinar las dinámicas de poder y competencia entre Estados en el ciberespacio, identificando las principales amenazas y oportunidades para Colombia en el ámbito de la defensa

Dinámicas de poder en el Ciberespacio

El ciberespacio se ha consolidado como un dominio fundamental en la arena geopolítica contemporánea, trascendiendo su concepción inicial como una mera red de interconexión tecnológica para erigirse en una infraestructura crítica y un teatro de interacciones entre estados. La capacidad de este dominio para transformar sociedades, influir en economías y políticas, y afectar la seguridad y defensa de las naciones lo convierte en un espacio estratégico de primer orden. En este contexto, la seguridad nacional se ve intrínsecamente ligada a la comprensión y el dominio del ciberespacio, especialmente para países como Colombia, que se enfrentan a un panorama de amenazas cibernéticas en constante evolución. La necesidad de analizar las dinámicas de poder y la competencia entre estados en el ámbito digital, así como de identificar las principales amenazas y oportunidades para la defensa nacional, se vuelve imperiosa para garantizar la soberanía y la estabilidad del país.

El estudio de las dinámicas de poder en el ciberespacio revela una notable transformación de los conceptos tradicionales de poder en el entorno digital. La influencia ya no se limita a la capacidad militar física, sino que se extiende a la habilidad para moldear percepciones y controlar el flujo de información y las narrativas en línea. En este sentido, la construcción de narrativas políticas a través de la cultura visual en redes sociales se erige como una herramienta clave para el ejercicio del poder, permitiendo a los actores influir en las creencias y comportamientos de audiencias tanto a nivel nacional como internacional (Acevedo, 2024). Esta capacidad de moldear la opinión pública y movilizar el apoyo o la oposición a determinadas políticas o líderes demuestra la creciente importancia del ciberespacio como un campo de batalla por la legitimidad y la influencia política.

Asimismo, la relación entre los ciudadanos y los gobiernos en los ecosistemas digitales plantea interrogantes fundamentales sobre la soberanía digital, los derechos digitales y el alcance

del control gubernamental sobre la información en línea (Jiménez-Varón, 2023). La propia definición del ciberespacio y la conceptualización de la ciberciudadanía como objetos de estudio en el ámbito de la comunicación y la educación subrayan la importancia de la información y la formación en la comprensión y la navegación del mundo digital, elementos cruciales para mantener o desafiar las estructuras de poder existentes (Jiménez-Varón, 2023). En un mundo cada vez más interconectado, la capacidad de acceder, utilizar y analizar la información se convierte en una fuente de poder en sí misma, lo que plantea desafíos sobre la equidad en el acceso a la información y la protección de la privacidad de los ciudadanos.

La competencia entre estados en el ciberespacio trasciende las confrontaciones militares convencionales, manifestándose en formas como el ciberespionaje, las operaciones de influencia y el desarrollo de capacidades cibernéticas ofensivas. El ciberespionaje, por ejemplo, permite a los estados obtener información sensible de otros países, incluyendo secretos de Estado, propiedad intelectual y datos personales, lo que puede proporcionar ventajas estratégicas en diversos ámbitos. Las operaciones de influencia, por otro lado, buscan manipular la opinión pública en otros países a través de la difusión de desinformación, propaganda y noticias falsas, lo que puede desestabilizar sociedades y socavar la confianza en las instituciones democráticas.

El desarrollo de capacidades cibernéticas ofensivas, finalmente, otorga a los estados la capacidad de llevar a cabo ataques cibernéticos contra la infraestructura crítica de otros países, lo que puede causar daños significativos y paralizar servicios esenciales. La necesidad de establecer un orden jurídico internacional para el ciberespacio surge de las limitaciones de las leyes tradicionales para abordar las características únicas del dominio digital, donde las acciones estatales pueden ser difíciles de atribuir y encubrir (Robles-Carrillo, 2016). La falta de un marco legal claro y vinculante a nivel internacional dificulta la regulación de las actividades cibernéticas de los estados y la rendición de cuentas por los ataques cibernéticos.

La distinción entre la soberanía tradicional y la soberanía digital refleja el creciente reconocimiento de que el control sobre la infraestructura digital, los datos y las actividades en línea dentro de las fronteras de una nación se está convirtiendo en un aspecto crítico de la soberanía nacional en el siglo XXI (Robles-Carrillo, 2023). La soberanía digital implica la capacidad de un Estado para ejercer control sobre su propio ciberespacio, incluyendo la regulación del flujo de información, la protección de los datos de los ciudadanos y la gestión de la infraestructura crítica. Este concepto desafía la noción tradicional de soberanía territorial, ya que el ciberespacio no

reconoce las fronteras físicas y las actividades en línea pueden tener un impacto transfronterizo. El debate en torno al concepto de arma cibernética es fundamental para comprender el potencial de escalada y conflicto en el ciberespacio, ya que la definición de lo que constituye un arma cibernética es esencial para establecer reglas de enfrentamiento y medidas de control de armamentos en el dominio digital (Robles-Carrillo, 2016). La falta de consenso sobre la definición de arma cibernética dificulta la negociación de tratados internacionales que regulen su uso y proliferación.

En última instancia, la conexión directa entre las relaciones internacionales, la geopolítica, el conflicto y el poder en el ciberespacio reafirma que las actividades cibernéticas no son incidentes técnicos aislados, sino que forman parte integral de la dinámica más amplia de las interacciones estatales y la competencia estratégica en la era moderna (Mata-Sánchez, 2023). El ciberespacio se ha convertido en un nuevo campo de batalla donde los estados compiten por el poder, la influencia y la seguridad, utilizando una variedad de herramientas y estrategias cibernéticas. Esta competencia tiene implicaciones significativas para la estabilidad internacional, ya que los ataques cibernéticos pueden desencadenar conflictos entre estados y erosionar la confianza mutua.

Amenazas y oportunidades para Colombia en el Ciberespacio

El análisis de las amenazas cibernéticas que enfrenta Colombia pone de manifiesto la importancia de un enfoque nacional para comprender y mitigar estos riesgos. Investigaciones específicas sobre las amenazas cibernéticas a la seguridad y defensa nacional en el contexto colombiano indican una preocupación prioritaria por aquellos riesgos que podrían afectar las funciones centrales del estado colombiano, sus capacidades militares y su soberanía nacional (Realpe & Cano, 2020). Entre estas amenazas se destacan los ataques a la infraestructura crítica, como las redes de energía, los sistemas de transporte y las instituciones financieras, que podrían tener consecuencias devastadoras para la economía y la seguridad del país. También se incluyen el ciberespionaje, que busca obtener información confidencial del gobierno y las empresas, y las operaciones de influencia, que intentan manipular la opinión pública y desestabilizar el orden político.

La identificación del "Compromiso por Correo Electrónico Empresarial" (BEC, por sus siglas en inglés) como una amenaza cibernética significativa en Colombia señala los riesgos económicos y de seguridad financiera asociados con los ataques cibernéticos dirigidos a empresas

y organizaciones en el país (Realpe et al, 2024). El BEC es un tipo de fraude en el que los ciberdelincuentes se hacen pasar por altos ejecutivos o proveedores de una empresa para engañar a los empleados y lograr que realicen transferencias de dinero no autorizadas. Este tipo de ataque puede causar pérdidas financieras significativas a las empresas y dañar su reputación. La cooperación policial internacional se vuelve crucial en este contexto, dada la naturaleza transfronteriza de muchas de estas amenazas (Realpe et al 2024). La colaboración entre las agencias de seguridad de diferentes países permite compartir información sobre las ciberamenazas, rastrear a los ciberdelincuentes y llevarlos ante la justicia.

El desarrollo de grupos nacionales de alerta, vigilancia y prevención subraya un enfoque proactivo por parte de Colombia para construir capacidad interna para identificar, monitorear y responder a las amenazas cibernéticas contra sus intereses nacionales (Herrera, 2015). Estos grupos desempeñan un papel fundamental en la detección temprana de los ataques cibernéticos, la investigación de los incidentes y la coordinación de la respuesta. También son responsables de la difusión de información sobre las ciberamenazas y las mejores prácticas de ciberseguridad a las entidades públicas y privadas. La creación de estos grupos especializados indica un esfuerzo estratégico para mejorar la resiliencia cibernética de Colombia y su capacidad para proteger su infraestructura crítica y sus intereses de seguridad nacional en el dominio digital (Herrera, 2015). La resiliencia cibernética se refiere a la capacidad de un sistema o una organización para resistir, recuperarse y adaptarse a los efectos adversos de los ataques cibernéticos.

El ciberespacio no solo presenta amenazas, sino también oportunidades estratégicas para fortalecer las capacidades de defensa de Colombia. La intersección del ciberespacio, la innovación tecnológica y los minerales críticos sugiere que Colombia, como parte de América Latina y el Caribe, debe considerar las implicaciones de ciberseguridad para sus recursos críticos y las oportunidades para aprovechar la tecnología en su protección y defensa en el ámbito digital (Barrera, 2023). Los minerales críticos, como el litio, el cobalto y las tierras raras, son esenciales para el desarrollo de las tecnologías emergentes, como los vehículos eléctricos, las energías renovables y los dispositivos electrónicos. Colombia posee importantes reservas de estos minerales, lo que la convierte en un actor clave en la economía global. Sin embargo, la explotación y el procesamiento de estos minerales también pueden exponer al país a ciberamenazas, como el espionaje industrial y el sabotaje. Por lo tanto, es fundamental que Colombia implemente medidas

de ciberseguridad robustas para proteger sus recursos críticos y aprovechar las oportunidades que ofrecen las nuevas tecnologías.

La aplicación de la inteligencia cibernética para contrarrestar amenazas e identificar oportunidades indica que Colombia puede mejorar su seguridad nacional aprovechando la vasta cantidad de información disponible en el ciberespacio para la detección de amenazas, el análisis y la toma de decisiones estratégicas en el ámbito de la defensa (Payá-Santos & Luque-Juárez, 2021). La inteligencia cibernética implica la recopilación, el análisis y la difusión de información sobre las ciberamenazas y los ciberactores, lo que permite anticipar los ataques, identificar las vulnerabilidades y desarrollar estrategias de defensa más efectivas. Colombia puede utilizar la inteligencia cibernética para proteger su infraestructura crítica, combatir el cibercrimen y apoyar las operaciones militares.

La existencia de una revista especializada como Revista Ciberespacio, Tecnología e Innovación de la Escuela Superior de Guerra, con un número significativo de artículos recientes dedicados a la ciberdefensa en Colombia, incluyendo temas como la inteligencia artificial, la gestión de riesgos y la protección de la infraestructura crítica, demuestra un enfoque académico e institucional nacional fuerte y continuo en el desarrollo de capacidades de ciberdefensa (Revista Ciberespacio, Tecnología e Innovación). Esta revista proporciona una plataforma para el intercambio de conocimientos y experiencias entre los investigadores, los profesionales y los responsables de la formulación de políticas en el campo de la ciberseguridad. Este compromiso se refleja también en la exploración del potencial de tecnologías emergentes como la inteligencia artificial y los conceptos del metaverso para ofrecer enfoques novedosos a la ciberdefensa y la planificación estratégica para Colombia (Barrera, 2023). La inteligencia artificial puede utilizarse para automatizar la detección y la respuesta a los ataques cibernéticos, mientras que el metaverso puede proporcionar un entorno virtual para la simulación de escenarios de ciberguerra y la formación de los profesionales de la ciberseguridad.

El panorama geopolítico del ciberespacio revela un nuevo campo de actuación para diversos actores, tanto estatales como no estatales. La concepción del ciberespacio como un nuevo campo de acción para el crimen organizado en América Latina subraya la naturaleza transnacional de las amenazas cibernéticas y la necesidad de cooperación regional para abordarlas, especialmente para Colombia dentro del contexto latinoamericano (Gazapo, 2017). El crimen organizado utiliza el ciberespacio para llevar a cabo una variedad de actividades delictivas, como el robo de datos, el

fraude en línea, la extorsión y el lavado de dinero. Estas actividades pueden tener un impacto significativo en la seguridad y la estabilidad de los países de la región. La transición del terrorismo al ciberespacio indica que los actores no estatales están utilizando cada vez más el dominio digital para la propaganda, el reclutamiento y potencialmente la planificación operativa, lo que plantea desafíos de seguridad únicos para Colombia (Gazapo, 2015).

Los grupos terroristas utilizan Internet para difundir su ideología, reclutar nuevos miembros, recaudar fondos y coordinar ataques. Esto requiere que Colombia desarrolle capacidades para monitorear y contrarrestar las actividades terroristas en el ciberespacio. La conceptualización del "Cyberscape" como un campo para la confrontación contemporánea sugiere que la ciberseguridad no es solo una cuestión técnica, sino un dominio de interacción estratégica y potencial conflicto entre actores internacionales, con implicaciones para la política exterior y la estrategia de defensa de Colombia (Gazapo, 2015). El ciberespacio se ha convertido en un nuevo escenario de competencia entre los estados, donde se llevan a cabo operaciones de espionaje, sabotaje e influencia. Esto plantea desafíos para la diplomacia y la seguridad internacional, ya que los ataques cibernéticos pueden desencadenar conflictos entre los países.

El papel de Internet como catalizador del terror enfatiza aún más el desafío de la radicalización en línea y la necesidad de que Colombia desarrolle estrategias para contrarrestar el contenido extremista y prevenir el uso de Internet para fines terroristas dentro de sus fronteras (Gazapo, 2018). La radicalización en línea es un proceso por el cual los individuos adoptan creencias y comportamientos extremistas a través de su exposición a contenido extremista en Internet. Esto puede llevar a la violencia y el terrorismo, lo que representa una amenaza para la seguridad nacional. Colombia debe implementar medidas para monitorear y eliminar el contenido extremista en línea, así como para educar al público sobre los riesgos de la radicalización. La descripción del ciberespacio como un escenario de conflicto subraya la comprensión de que las tensiones y rivalidades internacionales se están desarrollando cada vez más en el dominio digital, lo que requiere que Colombia esté preparada para posibles ataques cibernéticos y otras formas de agresión digital (Ágreda, 2012).

[T1] Desarrollo del objetivo 2

Identificar las vulnerabilidades y amenazas a la seguridad nacional de Colombia en el ciberespacio, evaluando su impacto potencial en las operaciones militares y la estabilidad del país.

Vulnerabilidades y amenazas a la Seguridad Nacional de Colombia en el Ciberespacio

La concepción de la seguridad nacional de Colombia, dentro del ámbito del ciberespacio, trasciende la mera protección de datos; implica la salvaguarda de la infraestructura crítica, la integridad de las operaciones gubernamentales y el bienestar general de la sociedad. Esta visión integral demanda una defensa robusta frente a los ciberataques susceptibles de comprometer la soberanía, la estabilidad económica y el orden social de la nación. En este contexto, el "ciberpoder", un concepto explorado extensamente en la literatura académica, se entrelaza de manera fundamental con la capacidad de Colombia para defender sus intereses en el dominio digital y proyectar influencia en el ciberespacio. Sin embargo, Colombia se enfrenta a un escenario complejo, moldeado por una historia de conflicto interno y un panorama tecnológico en desarrollo, factores que pueden exacerbar ciertas vulnerabilidades y plantear desafíos singulares para la protección de su seguridad nacional en el entorno digital. En particular, (Cano-Martínez, 2022) destaca la importancia de analizar la "Prospectiva de ciberseguridad nacional para Colombia a 2030", considerando diversos factores para comprender y abordar los retos en este ámbito.

Del Espectro de amenazas a la Infraestructura Crítica: Un Análisis Sectorial

La infraestructura crítica colombiana, entendida como el conjunto de sistemas y activos esenciales para la seguridad nacional, la economía y el funcionamiento básico de la sociedad, se ha convertido en un objetivo prioritario para una amplia gama de ciberamenazas. Este conjunto abarca sectores de vital importancia como el energético, el transporte y el financiero, cuya disrupción o sabotaje podría acarrear consecuencias devastadoras a escala nacional.

En el sector energético, por ejemplo, Colombia se enfrenta a un abanico diverso de ciberamenazas, que incluye desde actores de amenazas persistentes avanzadas (APT) hasta delincuentes cibernéticos y hacktivistas. Los ataques de denegación de servicio distribuido (DDoS) y el spear phishing representan peligros comunes. La vulnerabilidad de este sector se ve

intensificada por la inversión insuficiente en la gestión de los riesgos digitales y la lentitud en la modernización de la infraestructura y el software de los procesos. Como se señala en el análisis prospectivo de (Cano-Martínez, 2022), los resultados se agrupan en seis factores (político, económico, social, tecnológico, ecológico y legal) para ofrecer "una visión integrada útil para comprender y abordar el reto de la protección del Estado y la resiliencia de las organizaciones frente a la transformación digital". Esta perspectiva subraya la necesidad de una estrategia integral para proteger el sector energético, considerando no solo los aspectos tecnológicos, sino también los factores políticos, económicos y sociales que influyen en su vulnerabilidad. Además, (Ospina Díaz & Sanabria Rangel, 2020) examinan incidentes cibernéticos a nivel mundial y presentan un análisis del panorama colombiano en cuanto a seguridad digital, incluyendo la legislación y las acciones gubernamentales, lo cual complementa la visión prospectiva con un análisis del estado actual y las medidas tomadas.

El sector del transporte tampoco escapa a los riesgos cibernéticos. La creciente dependencia de los sistemas interconectados y la proliferación de dispositivos del Internet de las Cosas (IoT) en este sector han expandido la superficie de ataque y generado nuevas vulnerabilidades. Ataques de ransomware, phishing y vulnerabilidades en los sistemas IoT constituyen amenazas significativas, y la falta de actualizaciones de seguridad y una gestión deficiente de las contraseñas incrementan aún más estos riesgos. Esta situación transforma al sector del transporte en un objetivo atractivo para los ciberdelincuentes, quienes buscan explotar las debilidades de los sistemas para provocar interrupciones operativas, comprometer la seguridad de los pasajeros o sustraer información valiosa. (Aguilar Molina & Balseca Manzano, 2024) proporcionan una revisión sistemática de las tendencias, desafíos y vulnerabilidades de los ataques cibernéticos en ambientes de desarrollo, lo cual es relevante dado el creciente uso de software y sistemas en el sector del transporte.

Las instituciones financieras, por su parte, afrontan un elevado volumen de ciberataques diarios, motivados principalmente por la obtención de beneficios económicos. El phishing, el malware y el ransomware figuran entre las amenazas más comunes que asedian al sector financiero, poniendo en peligro no solo los activos monetarios, sino también la información financiera confidencial de los clientes. Si bien la Superintendencia Financiera de Colombia (SFC) ha implementado medidas para abordar la ciberseguridad en el sector, la naturaleza dinámica y la constante evolución de las amenazas exigen una vigilancia y adaptación continuas. (Castro et al., 2023) analizan el riesgo de los ciberataques para Colombia, presentando casos recientes contra

entidades gubernamentales y otros sectores como el bancario, lo que ilustra la realidad de estas amenazas para el sector financiero colombiano.

La interconexión de la infraestructura crítica y el potencial de crisis sistémicas

Un aspecto fundamental que se debe considerar es la interconexión existente entre los diversos sectores de la infraestructura crítica. Tal como se señala en el informe, los ciberataques dirigidos a un sector de la infraestructura crítica pueden tener un impacto en otros sectores debido a su interconexión. Esta interdependencia implica que una vulnerabilidad en un sector, como el energético, puede ser aprovechada para afectar el funcionamiento de otros sectores, como el transporte o las comunicaciones, desencadenando una crisis sistémica a escala nacional. Un ataque coordinado que explote estas interconexiones podría acarrear consecuencias catastróficas, provocando disrupciones generalizadas, desestabilización social y económica, y un profundo menoscabo de la seguridad nacional.

El Ciberespacio como Escenario de Conflicto: Implicaciones para las Operaciones Militares.

Las fuerzas militares colombianas también se enfrentan a un panorama de ciberamenazas en constante transformación. Dada la naturaleza de la información que manejan y las operaciones críticas que llevan a cabo, se han convertido en un objetivo importante para los ciberataques. Estos ataques pueden tener como propósito comprometer la inteligencia militar, interrumpir el mando y control, y socavar las capacidades operacionales, lo que representa una seria amenaza para la defensa de la nación.

El impacto de los ciberataques no se limita al ámbito digital; pueden tener repercusiones directas en las operaciones militares convencionales. La interrupción de las comunicaciones, la desactivación de sistemas de armas o el compromiso de la planificación estratégica son escenarios posibles que podrían afectar la eficacia de las fuerzas militares en el campo de batalla. La creciente integración de las capacidades cibernéticas en las operaciones militares y el surgimiento de escenarios de guerra híbrida, donde se combinan tácticas convencionales y no convencionales, difuminan aún más las fronteras entre la guerra tradicional y la guerra cibernética. Esta evolución exige el desarrollo de nuevas doctrinas y estrategias para la defensa y la ofensiva en este nuevo escenario de conflicto. En este sentido, (Realpe & Cano, 2020) analizan las "Amenazas

Cibernéticas a la Seguridad y Defensa Nacional", identificando las ciberamenazas latentes y emergentes y proponiendo una estrategia militar de Ciberdefensa que permita responder a estas amenazas con una visión integral, sistémica y prospectiva. Además, (Torres, 2018) ofrece un panorama general sobre los esfuerzos de la comunidad internacional a favor de la ciberseguridad y analiza el ciberespacio como un escenario estratégico para la seguridad y defensa, lo cual proporciona un contexto internacional relevante para entender los desafíos que enfrentan las fuerzas militares colombianas.

El ciberespionaje y la recopilación de inteligencia en el ámbito militar representan una amenaza significativa, ya que permiten a los adversarios obtener una ventaja estratégica al acceder a información confidencial y planes de defensa. Las operaciones de interferencia cibernética se emplean cada vez más para recopilar inteligencia e influir en las operaciones del adversario, lo que subraya la importancia de proteger la información militar y fortalecer las capacidades de contrainteligencia en el ciberespacio.

Adicionalmente, el ciberespacio desempeña un papel cada vez más relevante en la guerra híbrida, donde los actores no estatales y los adversarios estatales combinan operaciones cibernéticas con tácticas militares tradicionales y campañas de desinformación para desestabilizar, influir y obtener ventajas. Las operaciones cibernéticas pueden utilizarse para socavar la confianza pública, sembrar la discordia y complementar las acciones militares cinéticas, mientras que la desinformación y la propaganda difundidas en línea pueden influir en la opinión pública y desestabilizar el panorama político.

Frente a estas amenazas, las fuerzas militares colombianas están implementando medidas y estrategias para defenderse de los ciberataques y proteger sus sistemas críticos. La adopción de herramientas como Darktrace para la detección y respuesta a amenazas, así como la colaboración con empresas estadounidenses para fortalecer la ciberseguridad militar, son ejemplos de los esfuerzos que se están llevando a cabo para reforzar la postura de ciberdefensa de las fuerzas militares.

Vulnerabilidades en los Sistemas de Información del Gobierno Colombiano

El gobierno colombiano, al igual que muchas otras administraciones a nivel global, depende cada vez más de los sistemas digitales para llevar a cabo una amplia gama de funciones. Esta

digitalización abarca desde la prestación de servicios públicos hasta la administración interna y la gestión de grandes volúmenes de datos. Si bien esta transformación digital promete mejoras significativas en eficiencia, accesibilidad y agilidad en la gestión pública, también introduce nuevas y complejas vulnerabilidades que pueden ser explotadas por actores malintencionados.

Ospina Díaz & Sanabria Rangel (2020) señalan la importancia de analizar los "Desafíos nacionales frente a la ciberseguridad en el escenario global", lo cual incluye una revisión de la situación en Colombia y un examen de incidentes cibernéticos a nivel mundial. Este análisis proporciona un contexto valioso para comprender las vulnerabilidades específicas que enfrentan los sistemas de información del gobierno colombiano, no solo en el ámbito nacional sino también en relación con las tendencias globales.

Entre las vulnerabilidades comunes identificadas en los sistemas de información del gobierno colombiano se encuentran la autenticación débil, la exposición de datos sensibles, las fallas de inyección y las configuraciones incorrectas. (Aguilar & Manzano, 2024) destacan la importancia de la ciberseguridad y la necesidad de preparación, innovación tecnológica y medidas preventivas para proteger la integridad de la información, lo cual es especialmente relevante para los sistemas gubernamentales que manejan datos sensibles y son cruciales para el funcionamiento del Estado.

Los ataques exitosos contra los sistemas gubernamentales pueden tener consecuencias de gran alcance. (Castro et al.,2023) advierten sobre el riesgo de los ciberataques para Colombia, presentando casos recientes que ilustran el impacto potencial en entidades gubernamentales. Las violaciones de datos, la interrupción de servicios esenciales y la pérdida de confianza pública son solo algunas de las posibles repercusiones. La protección de la información gubernamental no es solo una cuestión técnica, sino también política y social, ya que la integridad y disponibilidad de los servicios públicos y la confianza en las instituciones son fundamentales para la estabilidad del país.

El uso del Ciberespacio por actores no Estatales y la Estabilidad Nacional

El ciberespacio se ha convertido en un escenario donde no solo los Estados interactúan, sino también una variedad de actores no estatales, cuyas acciones pueden tener un impacto significativo

en la seguridad y estabilidad de un país. En el caso de Colombia, el uso del ciberespacio por grupos armados, organizaciones de ciberdelincuencia y hacktivistas plantea desafíos particulares.

Grupos armados no estatales en Colombia, como las disidencias de las FARC y el ELN, están utilizando el ciberespacio para diversas actividades. Según (Realpe & Cano, 2020), es fundamental considerar aquellos riesgos que podrían afectar las funciones centrales del Estado colombiano, sus capacidades militares y su soberanía nacional, lo cual incluye el uso del ciberespacio por parte de estos grupos para desestabilizar el país. El ciberespacio proporciona a estos actores un medio para eludir las fronteras físicas, difundir su ideología, reclutar nuevos miembros y coordinar acciones, lo que plantea desafíos únicos para la seguridad nacional.

Las organizaciones de ciberdelincuencia también desempeñan un papel importante al atacar a Colombia. Estas organizaciones llevan a cabo actividades como ataques de ransomware, fraude financiero y robo de datos, las cuales pueden tener un impacto negativo en la economía y la confianza pública. (Ospina & Sanabria, 2020) señalan la importancia de analizar el tema de la seguridad de la información frente a las ciberamenazas y revisar la situación en Colombia, lo cual es esencial para comprender la magnitud del desafío que representan estas organizaciones.

El hacktivismo, es decir, el uso del ciberespacio para llevar a cabo acciones de protesta o activismo, también tiene el potencial de generar disrupción en Colombia. Grupos hacktivistas pueden atacar sistemas gubernamentales o infraestructura crítica con fines ideológicos, lo que puede tener consecuencias políticas y sociales. (Aguilar & Balseca, 2024) subrayan la importancia de la ciberseguridad y la necesidad de preparación y medidas preventivas, lo cual es crucial para mitigar el impacto de estas acciones.

Un desafío importante en este contexto es la atribución de los ciberataques a actores no estatales específicos. El anonimato que ofrece el ciberespacio dificulta la identificación de los responsables, lo que a su vez complica la respuesta y la disuasión. La falta de claridad sobre quién está detrás de un ataque puede generar tensiones y dificultar la aplicación de la ley.

Además, los marcos jurídicos internacionales y los debates en torno a la responsabilidad de los Estados por las acciones de actores no estatales que operan desde su territorio son relevantes. Colombia ha expresado su posición nacional sobre la aplicación del derecho internacional al ciberespacio, lo cual refleja la importancia de este tema en el contexto de la seguridad nacional.

[T1] Desarrollo del objetivo 3

Evaluar las estrategias y políticas de Colombia para la seguridad y defensa en el ciberespacio, con énfasis en el rol de las Fuerzas Militares y la cooperación con países aliados.

Estrategias y políticas de Colombia para la Seguridad y Defensa en el Ciberespacio

La creciente importancia del ciberespacio como un dominio fundamental para la interacción social, la actividad económica y las operaciones militares ha elevado la ciberseguridad y la ciberdefensa a una prioridad crítica para la seguridad nacional en todo el mundo (Chenou, 2021). Colombia, al igual que otras naciones, se enfrenta a desafíos cada vez mayores derivados de las amenazas cibernéticas, que ponen en riesgo tanto la infraestructura crítica y la economía digital como la seguridad nacional y la estabilidad regional (Pacheco, 2012). En respuesta a estos desafíos, Colombia ha reconocido la necesidad de desarrollar estrategias y políticas robustas para proteger su ciberespacio, y este análisis se centra en estos esfuerzos, prestando especial atención al papel de las Fuerzas Militares y la cooperación establecida con países aliados (Ministerio de Defensa Nacional de Colombia, 2022).

Inicialmente, el enfoque de Colombia en ciberseguridad estuvo influenciado por la adopción de directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en 2015. Chenou (2021) destaca que esta adopción temprana llevó a una estrategia centrada en la gestión del riesgo digital, con el objetivo principal de facilitar el desarrollo de la economía digital. Sin embargo, con el tiempo, se ha reconocido la necesidad de una perspectiva más amplia que abarque no solo la seguridad económica, sino también la defensa nacional y la estabilidad social (Urbanovics, 2022).

Marco Normativo Nacional de Ciberseguridad de Colombia

El marco normativo de ciberseguridad de Colombia ha experimentado una evolución significativa, lo que refleja una comprensión cada vez mayor de la complejidad y la importancia del ciberespacio (Policía Nacional de Colombia, s.f.). La estrategia inicial se centró en la gestión del riesgo digital, impulsada en parte por la aspiración de Colombia de unirse a la OCDE (Chenou, 2021). Chenou (2021) también señala que la adopción de las directrices de la OCDE en 2015 condujo a un enfoque centrado en el mercado, priorizando el desarrollo de una economía digital**.**

No obstante, la perspectiva se ha ampliado para abarcar una visión más integral de la ciberseguridad. El Decreto 338 de 2022 (Departamento de Comercio de los Estados Unidos, 2024) establece la obligación para entidades públicas y privadas de implementar medidas para la protección de la infraestructura crítica, lo que demuestra un reconocimiento de la necesidad de salvaguardar los servicios esenciales del país. Además, se ha introducido una Política Nacional de Ciberseguridad con el objetivo de fortalecer la resiliencia cibernética de la nación (Ministerio de Defensa Nacional de Colombia, 2022).

Un análisis comparativo con otros países de la región (Urbanovics, 2022) revela que Colombia ha logrado avances importantes, pero también identifica áreas de mejora. (Urbanovics, 2022) analizó las estrategias de ciberseguridad de seis países latinoamericanos y destacó las fortalezas de Colombia en la legislación sobre ciberdelincuencia y la protección de datos personales. La "Política Nacional de Seguridad Digital" de 2016 se destaca como un documento clave en este desarrollo. Sin embargo, en comparación con países como Chile y Argentina, la estrategia colombiana podría ser menos holística, con oportunidades de mejora en la protección de servicios digitales y esenciales, así como en la promoción de la educación en ciberseguridad (OEA y Trend Micro, 2014).

La evolución de las Estrategias Nacionales de Ciberseguridad (NCS) en Colombia subraya este cambio de enfoque (Fundación Karisma, 2020). La política de 2020 reconoció una limitación de las NCS anteriores: la insuficiente participación de múltiples partes interesadas. La estrategia actual enfatiza la particular vulnerabilidad de los niños en línea, dada la alta tasa de ciberdelincuencia y los bajos niveles de protección cibernética infantil en el país. El desarrollo de la NCS de 2020 se basó en varios documentos de política pública emitidos por el gobierno desde

2011. Un objetivo principal ha sido la creación de un Equipo de Respuesta a Incidentes de Ciberseguridad (CSIRT), que operará dentro de los organismos gubernamentales existentes. La política de 2020 busca fomentar la confianza digital y la ciberseguridad, y se estableció un Plan de Acción y Seguimiento (PAS) para el período 2020-2022 para implementar estos objetivos. Este plan incluye indicadores, presupuestos estimados y cronogramas para medir el progreso.

La participación de múltiples partes interesadas ha sido un aspecto clave en el desarrollo de la política de 2020 (Fundación Karisma, 2020). La OCDE brindó apoyo y asesoramiento experto en este proceso. Se llevaron a cabo dos períodos de consulta en 2019, recibiendo cientos de comentarios de diversas entidades, y se organizaron mesas redondas con actores clave del ecosistema digital, incluyendo empresas privadas, ONG, proveedores de telecomunicaciones y la academia. Además, la NCS colombiana destaca la importancia de las iniciativas de Investigación, Desarrollo e Innovación (I+D+i) para generar soluciones de ciberseguridad y promover el desarrollo de la industria a nivel nacional. La educación también se considera fundamental para desarrollar la fuerza laboral necesaria en el sector de la ciberseguridad (Digi Americas Alliance y U.S. Chamber of Commerce, 2024).

Las Fuerzas Militares de Colombia y la Ciberdefensa

El Ministerio de Defensa de Colombia asigna una importancia considerable a la ciberseguridad y la ciberdefensa, integrándolas en su planificación estratégica y marco de políticas (Ministerio de Defensa Nacional de Colombia, 2022). Dentro de la estructura del Viceministerio para las Políticas de Defensa y Seguridad, se encuentran tanto los "Planes Estratégicos de Ciberseguridad y Ciberdefensa" como la "Política de Ciberseguridad y Ciberdefensa", lo que subraya el reconocimiento a nivel nacional del papel fundamental que desempeñan las fuerzas militares en la protección del ciberespacio.

Colombia está llevando a cabo esfuerzos activos para mejorar sus capacidades de ciberdefensa militar, invirtiendo en la construcción de nuevos Centros de Comando y Control en Bogotá y otras ciudades (Digi Americas Alliance, 2024), los cuales probablemente incorporarán infraestructura de ciberdefensa. Además, el gobierno ha manifestado su interés en adquirir material de ciberseguridad y desarrollar capacidades integradas de comunicaciones y ciberdefensa. Estos movimientos proactivos indican un compromiso por fortalecer la capacidad del ejército para

responder y disuadir las amenazas cibernéticas. La construcción de Centros de Comando y Control sugiere un esfuerzo por centralizar y coordinar las operaciones de ciberdefensa.

La política de ciberseguridad de Colombia de 2016 identifica la infraestructura cibernética como infraestructura crítica y promueve una estrategia de defensa para la misma (Policía Nacional de Colombia, s.f.). Esta designación implica un papel directo para las fuerzas militares en su protección, aunque los detalles específicos de esta función requieren una exploración más profunda. Es evidente que el gobierno colombiano considera la protección de su ciberespacio como una responsabilidad compartida entre diversas entidades, con un papel significativo asignado a las Fuerzas Militares en la defensa contra amenazas que puedan comprometer la seguridad nacional y la infraestructura esencial.

Cooperación Internacional en Ciberseguridad y Ciberdefensa

Colombia participa activamente en la cooperación internacional en materia de ciberseguridad con una variedad de socios, lo que refleja una comprensión de que la ciberseguridad es un desafío global que exige una acción colectiva (Urbanovics, 2022). Esta amplia red de asociaciones permite a Colombia aprovechar la experiencia y los recursos de diversos actores internacionales.

La cooperación con Estados Unidos parece centrarse en la ciberseguridad en general y en la resiliencia cibernética relacionada con la inteligencia artificial (Digi Americas Alliance y U.S. Chamber of Commerce, 2024). Un diálogo sobre IA y ciberseguridad en América Latina, liderado por Estados Unidos y con participación colombiana, destaca este enfoque. La relación con la OTAN también es significativa, ya que Colombia se convirtió en el primer socio latinoamericano de la organización en 2017 (NATO, 2024). La cooperación con la OTAN enfatiza la provisión práctica de seguridad y el abordaje de problemas globales, incluida la ciberseguridad. Además, la Unión Europea también ha mostrado interés en la cooperación en ciberseguridad con América Latina (Fonseca, 2025), lo que podría abrir nuevas vías de colaboración para Colombia.

La Organización de los Estados Americanos (OEA) desempeña un papel crucial en el apoyo al desarrollo de capacidades de ciberseguridad y en el fomento de la cooperación regional en América Latina (OEA, 2020), siendo Colombia un participante activo y beneficiario del apoyo de la OEA. Los informes de la OEA (OEA y Trend Micro, 2014) destacan la insuficiente preparación

de la región LAC, incluida Colombia, para los ataques cibernéticos y la necesidad de una mayor cooperación internacional. La participación de Colombia en iniciativas regionales como CSIRT Américas y sus formatos de cooperación demuestran su compromiso con el trabajo conjunto con sus vecinos para abordar desafíos cibernéticos compartidos.

Además de las asociaciones con organizaciones y países específicos, Colombia también está comprometida con marcos legales y operativos internacionales para combatir el cibercrimen. Su participación en la Fuerza de Tarea Conjunta contra el Cibercrimen (J-CAT) de Europol y sus esfuerzos por adherirse al Convenio de Budapest subrayan esta dedicación (Policía Nacional de Colombia, s.f.). Este enfoque en el cibercrimen refleja el reconocimiento de la necesidad de abordar tanto las amenazas patrocinadas por el estado como las actividades delictivas en el ciberespacio.

Estrategias de Ciberdefensa para la Protección de la Infraestructura Crítica en Colombia

Colombia ha reconocido la importancia fundamental de proteger su infraestructura crítica mediante la promulgación de decretos y la inclusión de esta protección en su política nacional de ciberseguridad (Departamento de Comercio de los Estados Unidos, 2024). Esta infraestructura, que abarca sectores esenciales como la energía, las telecomunicaciones, las finanzas y el transporte, es vital para el funcionamiento del país, y su protección contra ataques cibernéticos es una prioridad nacional.

El informe de la OEA y Trend Micro (2014) destaca que la infraestructura crítica en Colombia, al igual que en otras partes de América, enfrenta amenazas cibernéticas cada vez mayores. Esto subraya la necesidad de estrategias de protección efectivas y una colaboración más sólida entre el sector público y el privado. El diálogo y la cooperación proactiva entre el gobierno y las organizaciones privadas en relación con la ciberseguridad de la infraestructura crítica son esenciales, aunque el informe sugiere que existen brechas en esta colaboración.

La política de ciberseguridad de 2016 de Colombia identifica específicamente la infraestructura cibernética como crítica y promueve una estrategia de defensa para ella (Policía Nacional de Colombia, s.f.). Esto implica que se están implementando medidas para identificar, evaluar y mitigar los riesgos cibernéticos para estos activos esenciales. Sin embargo, la complejidad del panorama de amenazas y la creciente sofisticación de los ataques requieren una vigilancia constante y una adaptación continua de las estrategias de defensa (Digi Americas Alliance, 2024). La colaboración entre las entidades gubernamentales responsables y las empresas del sector

privado es crucial para garantizar una protección integral y eficaz de la infraestructura crítica de Colombia.

[T1] Conclusiones

La investigación desarrollada en este artículo permitió comprender con mayor profundidad la creciente centralidad del ciberespacio como dominio estratégico de competencia, conflicto y cooperación entre Estados, actores no estatales y estructuras híbridas. A través del análisis de las dinámicas de poder digital, las amenazas emergentes y las capacidades nacionales, se logró evidenciar que la seguridad y defensa en el ciberespacio no pueden seguir siendo tratadas como una extensión técnica o marginal de la política de seguridad nacional, sino como un eje estructural que requiere atención prioritaria, enfoque interinstitucional y visión geopolítica de largo plazo.

En primer lugar, el análisis de las dinámicas de poder y competencia interestatal en el ciberespacio revela que este dominio se ha convertido en un nuevo escenario de disputa por la influencia, la legitimidad y la capacidad de disuasión. Las potencias globales han incorporado capacidades cibernéticas ofensivas, operaciones de influencia digital y estrategias de ciberespionaje dentro de su arquitectura de poder. En este marco, Colombia no puede permanecer ajena a estas transformaciones. La soberanía digital, entendida como la capacidad de un Estado para proteger y gestionar su infraestructura crítica, sus datos y sus narrativas en línea, emerge como una condición imprescindible para la autonomía estratégica del país. Asimismo, la ausencia de un marco jurídico internacional vinculante en materia de ciberguerra y ciberataques representa un vacío que deja a los Estados medianos y pequeños, como Colombia, en una posición vulnerable frente a actores más sofisticados y agresivos.

El segundo objetivo permitió examinar con detenimiento las principales amenazas y vulnerabilidades que enfrenta Colombia en el ámbito digital. La evidencia muestra que sectores clave como el energético, el financiero, el transporte y las comunicaciones están expuestos a un abanico creciente de riesgos cibernéticos, desde ransomware y phishing hasta ataques de denegación de servicio (DDoS) y amenazas persistentes avanzadas (APT). Esta exposición no solo compromete la eficiencia de los servicios y la estabilidad económica, sino que puede escalar hacia escenarios de desestabilización social e incluso parálisis estatal si se afectan simultáneamente sistemas interconectados.

Adicionalmente, las Fuerzas Militares y los sistemas de inteligencia del país también están en la mira de posibles ciberataques, espionaje digital y campañas de desinformación que buscan socavar su capacidad operativa y afectar la toma de decisiones estratégicas. Este panorama se agrava con el uso del ciberespacio por parte de actores no estatales como el crimen organizado, los grupos armados ilegales y los colectivos hacktivistas, que emplean las redes digitales para difundir propaganda, reclutar simpatizantes, coordinar acciones y desinformar a la población. La capacidad de atribuir técnicamente estos ataques sigue siendo limitada, lo que complica tanto la disuasión como la sanción efectiva de los responsables.

Frente a este contexto desafiante, el tercer objetivo permitió identificar y evaluar los esfuerzos que ha desarrollado Colombia en materia de ciberseguridad y ciberdefensa, destacando avances importantes, pero también brechas estructurales. El país ha logrado consolidar un marco normativo básico, ha formulado estrategias nacionales de ciberseguridad, y ha promovido la articulación de actores públicos y privados en torno a la protección de infraestructura crítica. Se han creado centros de respuesta a incidentes (CSIRT), se han fortalecido las capacidades militares en ciberdefensa, y se han establecido mecanismos de cooperación internacional con aliados como Estados Unidos, la OTAN, la Unión Europea y la OEA.

Sin embargo, la investigación también señala la necesidad de fortalecer la implementación efectiva de estas políticas, superar la fragmentación institucional, garantizar recursos sostenibles para el desarrollo tecnológico nacional, y promover una cultura cibernética transversal que incluya la educación ciudadana, la capacitación del talento humano y la innovación en inteligencia artificial aplicada a la defensa. El rol de las Fuerzas Militares debe consolidarse desde una doctrina clara que comprenda al ciberespacio no solo como un ámbito técnico, sino como un teatro de operaciones con implicaciones tácticas, operacionales y estratégicas. Esto exige también la integración del pensamiento cibernético en la planeación militar y en la formación de sus cuadros estratégicos.
Desde una perspectiva regional, Colombia tiene la oportunidad de convertirse en un referente latinoamericano en ciberseguridad, articulando esfuerzos multilaterales, promoviendo normas comunes y cooperando en la lucha contra amenazas transnacionales. La estabilidad del país en el entorno digital dependerá no solo de sus capacidades internas, sino de su habilidad para integrarse en redes de cooperación estratégica más amplias.

Finalmente, este trabajo evidencia que el ciberespacio no es un escenario ajeno a las lógicas tradicionales del poder y la geopolítica. Por el contrario, se ha constituido en una nueva frontera

donde se disputan recursos, información, influencia y legitimidad. La seguridad digital de Colombia, por tanto, no puede ser abordada desde una lógica exclusivamente reactiva o fragmentada. Se requiere una visión de Estado, transversal, articulada, moderna y anticipatoria, que entienda la defensa cibernética como un componente esencial de la soberanía nacional y de la protección de los ciudadanos frente a los riesgos de una era cada vez más interconectada, compleja y conflictiva.

[T1] Referencias (APA séptima edición)

- Acevedo, ED. (2024). Símbolos y Poder: La construcción de narrativas políticas a través de la cultura visual en las redes sociales.
- Acevedo, ED. (2022). El homo connected y gobiernos en América Latina: Ciudadanías en ecosistemas digitales.
- Ágreda, Á. G. de (2012). El ciberespacio como escenario del conflicto.
- Barrera, C. (2023). Ciberespacio, innovación tecnológica y minerales críticos: Retos y oportunidades para América Latina y el Caribe. Revista del Ejército, Fuerza Aérea y Guardia Nacional.
- Barrinha, A., & Renard, T. (2017). Cyber-security and international relations: analytical approaches and policy implications. Global Affairs, 3(1), 23-33.
- Buchanan, B. (2017). The cybersecurity dilemma: hacking, espionage, and the future of warfare. Oxford University Press.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.
- Castillo-Pulido, L. E., Realpe, M. E., Cano, J., & Jiménez-Acosta, J. F. (2024). Amenazas cibernéticas a la seguridad y defensa nacional: Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email Compromise. Revista Logos Ciencia & Tecnología.
- Constitución Política de Colombia [Const.]. (1991).
- Deibert, R. J. (2013). Black code: Surveillance, privacy, and the dark side of the Internet. Signal.

- Gazapo, M. J. (2015). Terrorism And Tts Transition To Cyberspace. 2015 European Intelligence and Security Informatics Conference.
- Gazapo, M. J. (2015). Cyberscape: Cybersecurity as a Field for Contemporary Confrontation. International Scientific Conference Strategies XXI - The Complex And...
- Gazapo, M. J. (2017). Ciberespacio: El Nuevo Campo De Actuación Del Crimen Organizado En América Latina. El Crimen Organizado En América Latina: Manifestaciones, Facilitadores y ...
- Gazapo, M. J. (2018). Internet Como Catalizador Del Terror: El Uso Del Ciberespacio Por Parte De
- Giles, K. (2016). Handbook of Russian information warfare. NATO Defense Collage.
- Gómez de Agreda, Á. (2012). El Ciberespacio como entorno social y de conflicto. Instituto Español de Estudios Estratégicos.
- Herrera, CAP. (2015). Desarrollo de grupos nacionales de alerta, vigilancia y prevención frente a amenazas cibernéticas. la multidimensionalidad de la seguridad nacional: retos y desafíos d
- Jesson, J., Matheson, L., & Lacey, F. M. (2011). Doing your literature review: Traditional and systematic techniques. SAGE.
- Jiménez-Varón, V. A. Y. P. (2023). El ciberespacio y las ciberciudadanías como objetos de estudio de la comunicación-educación. Desarrollo Regional. La universidad al servicio de las regiones.
- Kanuck, S. (2018). Cyber sovereignty: The quest for order in a contested domain. Orbis, 62(2), 205-221.
- Krippendorff, K. (2018). Content analysis: An introduction to its methodology (4th ed.). SAGE Publications.
- Ley 1273 de 2009. Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. 16 de enero de 2009. DO: 47.287.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17-de octubre de 2012. DO: 48.587.
- Lindsay, J. R. (2015). The impact of technological innovation on the future character of conflict. Joint Force Quarterly, 78(3), 56-65.
- Mata-Sánchez, G. (2023). Relaciones internacionales y geopolítica: conflicto y poder en el ciberespacio. Brazilian Journal of Law & International Relations/Relações Internacionais.
- Medina-Ochoa, G. E. (2019). La Seguridad en el Ciberespacio: Un desafío para Colombia. Sello Editorial ESDEG. https://doi.org/10.25062/9789585216549

- Ministerio de Defensa Nacional de Colombia. (2016). Política de Defensa y Seguridad (PDS). Ministerio de Defensa Nacional.
- Mirón, M. (2019). La guerra irregular, insurgencias y cómo contrarrestarlas. Revista Científica General José María Córdova, 17(27), 457-480. https://doi.org/10.21830/19006586.497
- Nakashima, E. (2011). Cyber warfare: How conflicts in cyberspace are challenging America and changing the world. PublicAffairs.
- Organización de los Estados Americanos. (2011). Estrategia de ciberseguridad de la OEA. OEA.
- Organizaciones Terroristas. Conflictos Y Diplomacia, Desarrollo Y Paz, Globalización Y Medio Ambiente.
- Patton, M. Q. (2015). Qualitative research & evaluation methods: Integrating theory and practice. SAGE.
- Payá-Santos, C., & Luque-Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. Revista Científica General José María Córdova. https://dx.doi.org/10.21830/19006586.855
- Realpe, M., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. Seguridad Informática [congreso] X Congreso Iberoamericano. Universidad del
- Rid, T. (2013). Cyber war will not take place. Oxford University Press.

- Robles-Carrillo, M. (2016). El ciberespacio: Presupuestos para su ordenación jurídico-internacional.
- Revista Chilena de Derecho y Ciencia Política. https://doi.org/10.7770/rchdcp-V1N1-art1025
- Robles-Carrillo, M. (2016). El concepto de arma cibernética en el marco internacional: una aproximación funcional. bie3: ieee.
- Robles-Carrillo, M. (2023). Sovereignty vs. Digital Sovereignty. Journal of Digital Technologies and Law. https://doi.org/10.21202/jdtl.2023.29
- Wendt, A. (1999). Social theory of international politics. Cambridge University Press.