El tridente estratégico en Colombia: integración de ciberseguridad, inteligencia y fuerzas especiales para fortalecer la defensa nacional.

Mayor Leon Osorio Diego

Artículo para optar al título profesional:

Magister en Seguridad y Defensa Nacional

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

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Leon Osorio Diego
Identificación	**:**	1047364285
Programa académico	**:**	Maestría en Seguridad y Defensa
Tutor metodológico	**:**	DO. Jonnathan Jiménez Reina
Tutor temático	**:**	BG (Rva) Flórez Cuervo Raul
Fecha de entrega	**:**	26 de agosto de 2024
Extensión	**:**	7935 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 articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

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

El tridente estratégico en Colombia: integración de ciberseguridad, inteligencia y fuerzas especiales para fortalecer la defensa nacional.

The Strategic Trident in Colombia: Integration of Cybersecurity, Intelligence and Special Forces to Strengthen National Defense.

Diego León Osorio[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La seguridad nacional de Colombia enfrenta desafíos crecientes debido a la evolución de amenazas híbridas, cibernéticas y transnacionales. Este artículo analiza la necesidad de integrar tres capacidades clave del sector defensa: la ciberseguridad, la inteligencia militar y las fuerzas especiales, bajo un modelo sinérgico denominado "tridente estratégico". A partir de una metodología cualitativa y un análisis documental, se identifican los avances, limitaciones y retos en la articulación de estas capacidades, tanto a nivel doctrinal como operativo. El estudio compara experiencias internacionales con el contexto colombiano y propone una ruta estratégica para consolidar una defensa nacional más efectiva, anticipativa y coordinada. La investigación concluye que la integración de estos tres pilares es esencial para enfrentar los escenarios de guerra contemporánea y fortalecer la resiliencia del Estado ante amenazas complejas.
Palabras clave: Ciberseguridad; Defensa híbrida; Integración estratégica; Inteligencia militar; Fuerzas especiales; Seguridad nacional.

Abstract: Colombia's national security faces growing challenges due to the evolution of hybrid, cyber, and transnational threats. This article analyzes the need to integrate three key capabilities in the defense sector: cybersecurity, military intelligence, and special forces, under a synergistic model known as the "strategic trident." Using a qualitative methodology and documentary analysis, the article identifies the advancements, limitations, and challenges in the integration of these capabilities, both at the doctrinal and operational levels. The study compares international experiences with the Colombian context and proposes a strategic path to consolidate a more effective, anticipatory, and coordinated national defense. The research concludes that the integration of these three pillars is essential to face contemporary warfare scenarios and to strengthen the resilience of the State against complex threats.
Keywords: Cybersecurity; Hybrid Defense; Military Intelligence; National Security; Special Forces; Strategic Integration.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en seguridad y defensa nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2441-2299 Contacto: diego.leon@esdeg.edu.co.

Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C., Colombia

[T1] Introducción

La seguridad nacional de Colombia enfrenta un entorno cada vez más complejo debido a la evolución de las amenazas híbridas y cibernéticas. Si bien el país ha desarrollado capacidades militares sólidas en la lucha contra insurgencias internas, el panorama actual exige una adaptación a nuevas formas de conflicto, donde los adversarios operan en el ciberespacio y emplean tácticas irregulares (Montero Moncada, 2020). En este contexto, la fragmentación entre tres capacidades clave –ciberseguridad, inteligencia militar y fuerzas especiales– representa una debilidad estratégica para la defensa nacional. Cada una de estas áreas ha operado históricamente de manera autónoma, lo que ha limitado su capacidad de respuesta integral frente a las amenazas emergentes (Peña Peña y Olaya Murcia, 2020).

El problema central de este estudio radica en la falta de una doctrina consolidada que articule estas tres capacidades en un modelo operativo sinérgico. A pesar de los avances normativos y tecnológicos en materia de ciberseguridad y operaciones especiales, la ausencia de una integración efectiva impide aprovechar al máximo las ventajas que ofrece cada componente (Rodríguez y Garzón, 2024). De allí se desprende la pregunta de investigación que orienta este artículo: ¿de qué manera la integración de las capacidades de ciberseguridad, inteligencia y fuerzas especiales puede fortalecer la defensa nacional de Colombia frente a las amenazas contemporáneas? Esta preocupación no es exclusiva del caso colombiano: en América Latina los delitos cibernéticos transnacionales se han incrementado significativamente, afectando infraestructura crítica y la seguridad nacional (UNODC, 2022).

Diversas experiencias internacionales han demostrado la eficacia de este enfoque. Países como Estados Unidos, Rusia y China han desarrollado modelos estratégicos en los que la combinación de inteligencia, operaciones especiales y capacidades cibernéticas

conforma la primera línea de defensa ante conflictos híbridos (Le Billon et al., 2020). Por ejemplo, el ejército estadounidense ha implementado una doctrina de "triada estratégica", que vincula sus fuerzas de operaciones especiales con el dominio cibernético, ampliando su espectro de acción tanto en ofensiva como en defensiva (Montero Moncada, 2020). En el marco de la OTAN, la articulación entre inteligencia, ciberseguridad y fuerzas especiales ha permitido una respuesta más efectiva ante amenazas como el terrorismo internacional y la guerra cibernética, lo que evidencia la pertinencia de este enfoque para Colombia (Peña Peña y Olaya Murcia, 2020).

En el caso colombiano, se han desarrollado iniciativas para fortalecer cada una de estas capacidades de manera individual. En materia de ciberseguridad y ciberdefensa, el país fue pionero en América Latina con la creación de una política nacional específica (CONPES 3701 de 2011), lo que permitió el establecimiento del Comando Conjunto Cibernético de las Fuerzas Militares y el Equipo de Respuesta a Emergencias Cibernéticas (ColCERT) (Cáceres García, 2017). A nivel de inteligencia militar, la evolución doctrinal ha mejorado los procesos de recolección, análisis y contrainteligencia con un enfoque más preventivo y adaptado a las nuevas amenazas del ciberespacio (Gómez, 2017). En cuanto a las fuerzas especiales, su papel ha sido fundamental en operaciones de alto valor estratégico, como rescates y ataques quirúrgicos, aunque aún presentan desafíos en la adaptación a escenarios digitales (Rodríguez y Garzón, 2024).

A pesar de estos avances, persisten brechas en la integración efectiva de estos componentes. Rodríguez y Garzón (2024) destacan que las unidades de fuerzas especiales deben incorporar el dominio digital en su doctrina de combate, preparándose para operar en el ciberespacio con las mismas capacidades con las que enfrentan amenazas físicas. Asimismo, Peña Peña y Olaya Murcia (2020) sostienen que la sinergia entre inteligencia,

ciberseguridad y fuerzas especiales puede mejorar significativamente la efectividad de las Fuerzas Militares colombianas en escenarios de guerra híbrida. Sin embargo, esta integración requiere un marco doctrinal y operacional claro, que permita la interoperabilidad entre estas capacidades estratégicas.

En este punto, resulta indispensable incorporar un marco teórico que dé sustento a la investigación. Desde la perspectiva del neorrealismo (Waltz, 2000), el Estado opera en un sistema internacional anárquico donde la supervivencia es el objetivo principal. Bajo esta lógica, la ciberseguridad, la inteligencia y las fuerzas especiales no son simples herramientas de poder ofensivo, sino capacidades esenciales para garantizar la seguridad estatal. La cooperación internacional en estos ámbitos —como las alianzas de Colombia en inteligencia y ciberseguridad— puede interpretarse como una estrategia de alineamiento con potencias hegemónicas o con organismos multilaterales, cuyo fin último es reforzar la seguridad nacional.

De manera complementaria, el realismo defensivo (Walt, 1998) sostiene que la política exterior del Estado se rige por el equilibrio de amenazas. Así, las operaciones conjuntas en ciberseguridad, inteligencia y fuerzas especiales se orientan a mitigar riesgos y a prevenir que actores hostiles generen desequilibrios regionales. En este marco, la participación de Colombia en esquemas de cooperación como la OTAN o la MFO se entiende como parte de una política de seguridad colectiva, donde la interoperabilidad y el intercambio de capacidades buscan contrarrestar amenazas transnacionales.

Este estudio aborda dicha brecha doctrinal mediante un análisis sistemático sobre cómo la coordinación entre ciberseguridad, inteligencia y fuerzas especiales puede fortalecer la defensa nacional colombiana en el siglo XXI. La adopción de un modelo basado en el tridente estratégico permitiría una respuesta más ágil y efectiva ante las amenazas actuales,

asegurando que el país no solo se adapte a los desafíos contemporáneos, sino que también desarrolle una estrategia de defensa avanzada y coordinada.

[T1] Metodología

Este estudio se desarrolla bajo un enfoque cualitativo, con un diseño exploratorio y descriptivo, que permite analizar la integración de ciberseguridad, inteligencia y fuerzas especiales en la defensa nacional de Colombia. Se fundamenta en el análisis documental y en la revisión de literatura especializada para comprender cómo estos tres componentes pueden articularse estratégicamente frente a las amenazas contemporáneas.

El enfoque cualitativo es idóneo para esta investigación, dado que permite interpretar procesos, doctrinas y estrategias de defensa que no pueden ser reducidos a simples variables numéricas (Creswell y Creswell, 2018). A través de esta metodología, se busca comprender cómo la doctrina militar y las capacidades tecnológicas se han desarrollado en otros países, y cómo pueden adaptarse al contexto colombiano. Se prioriza la identificación de patrones en la literatura existente, estableciendo relaciones entre los conceptos de inteligencia, ciberseguridad y fuerzas especiales y su impacto en la seguridad nacional.

El diseño exploratorio y descriptivo permite no solo examinar la integración de estos elementos en otros escenarios internacionales, sino también evaluar el estado actual de su implementación en Colombia (Flick, 2018). Esto se logra mediante la revisión de fuentes primarias y secundarias, incluyendo documentos oficiales, doctrinas militares, informes gubernamentales, libros especializados y artículos científicos publicados en revistas indexadas.

Para la selección de fuentes, se empleó una estrategia de búsqueda sistemática en bases de datos académicas como Scopus, Web of Science, JSTOR y Google Scholar, así

como documentos de organismos especializados como la OTAN, la Escuela Superior de Guerra de Colombia y centros de investigación en defensa y seguridad. Se priorizaron estudios publicados en los últimos diez años, con excepción de documentos estratégicos clave que siguen siendo referenciales en el campo.

El análisis documental fue el principal método de recolección de información, siguiendo la propuesta de Bowen (2009), quien destaca que esta técnica permite identificar tendencias, patrones y enfoques dentro de los textos analizados. Se aplicó un proceso de codificación temática, categorizando la información en tres ejes principales: i) estrategias de integración de ciberseguridad, inteligencia y fuerzas especiales en defensa nacional; ii) experiencias internacionales en la implementación de un tridente estratégico de defensa; iii) estado actual de la ciberseguridad, la inteligencia militar y las fuerzas especiales en Colombia.

La interpretación de los hallazgos se realizó a partir del análisis comparativo de experiencias internacionales y su aplicabilidad al contexto colombiano. Se contrastaron las doctrinas militares de países con modelos avanzados en este ámbito, como Estados Unidos, Reino Unido e Israel, con la evolución de las Fuerzas Militares de Colombia en materia de integración estratégica.

Dado que esta investigación no involucra experimentación ni interacción con sujetos humanos, no requiere la aprobación de un comité de ética. Sin embargo, se respetaron los principios de rigor académico, transparencia en el uso de fuentes y validación de datos mediante la triangulación de información proveniente de distintas fuentes documentales.

[T1] Funciones, alcances y particularidades de ciberseguridad, inteligencia y fuerzas especiales en la seguridad nacional colombiana.

La seguridad nacional en Colombia ha experimentado una transformación significativa en las últimas décadas, impulsada por la evolución del conflicto armado interno, la creciente presencia de actores transnacionales y la aparición de nuevas amenazas asociadas al entorno digital. Si bien el país ha desarrollado una capacidad sólida para enfrentar desafíos tradicionales como el narcotráfico, la insurgencia y la criminalidad organizada, los escenarios actuales exigen respuestas adaptativas y multidimensionales. Las amenazas híbridas que combinan operaciones cibernéticas, guerra de información, sabotaje, terrorismo y conflicto armado no convencional— requieren un replanteamiento del modelo de defensa.

En este escenario, tres capacidades estratégicas emergen como componentes esenciales del aparato de seguridad nacional: la ciberseguridad, encargada de proteger la infraestructura crítica digital y garantizar la soberanía en el ciberespacio; la inteligencia militar, orientada a anticipar y neutralizar amenazas mediante el análisis estratégico; y las fuerzas especiales, dotadas de habilidades tácticas para ejecutar operaciones de alta precisión en entornos complejos. Cada una de estas funciones ha evolucionado de forma particular, con avances institucionales, normativos y operativos relevantes. No obstante, aún se observan brechas considerables en su articulación interinstitucional, lo que limita el aprovechamiento integral de sus capacidades.

Tabla 1.

Identificación de variables

Capacidad Estratégica	Fortaleza	Aspecto de mejora
Ciberseguridad	Creación del Comando Conjunto Cibernético (C4) y el Equipo de Respuesta a Emergencias	Falta de interoperabilidad con la inteligencia militar y las fuerzas especiales. Ausencia de una doctrina clara sobre el uso de

	Cibernéticas (ColCERT). A su vez la implementación de monitoreo y detección temprana para neutralizar ataques.	capacidades cibernéticas ofensivas en operaciones militares junto con la limitada cooperación interestatal en la región.
Inteligencia Militar	Se ha expandido su alcance de la guerra interna a las amenazas híbridas y del ciberespacio, esto a través de HUMINT, SIGINT y ciberinteligencia para identificar amenazas.	La rápida evolución de las tácticas de ataque cibernético dificulta la adaptación, a su vez los desafíos en la integración tecnológica y operativa para servir de puente entre la ciberseguridad y las unidades en campo.
Fuerzas Especiales	Configuración ante adaptabilididad contra GAO y fortalecimiento de operaciones conjuntas con inteligencia y ciberseguridad.	Carece de integración doctrinal entre las capacidades físicas y digitales y carece de una modernización insuficiente para operar en un entorno de guerra multidimensional y de adaptación a la guerra híbrida

Nota. Elaboración propia.

Este objetivo busca caracterizar en detalle las funciones, los alcances y las particularidades de estas tres capacidades dentro del sistema de seguridad y defensa de Colombia. Para ello, se examinan sus desarrollos recientes, los desafíos que enfrentan frente al contexto contemporáneo y el potencial que tienen si son integradas de manera doctrinal y operativa. Esta caracterización constituye la base para comprender la necesidad de avanzar hacia un modelo de defensa que responda de manera eficaz a la complejidad del entorno estratégico actual.

[T2] Ciberseguridad en la seguridad nacional

El ciberespacio ha sido reconocido como el quinto dominio de la guerra, junto con los ámbitos terrestre, marítimo, aéreo y espacial. Esto ha obligado a los Estados a redefinir sus estrategias de seguridad, dado que el ciberespacio es un escenario en el que grupos insurgentes, redes criminales y actores estatales hostiles pueden operar con un alto grado de anonimato y con un impacto estratégico significativo (Puyosa, 2021). En Colombia, la ciberseguridad es considerada un elemento fundamental dentro de la estrategia de defensa, con la creación de estructuras especializadas como el Comando Conjunto Cibernético (C4)

y el Equipo de Respuesta a Emergencias Cibernéticas (ColCERT) (Ministerio de Defensa Nacional [MDN], 2023).

La función principal de la ciberseguridad en la defensa nacional es garantizar la protección de la infraestructura crítica del país, incluyendo sistemas de telecomunicaciones, redes eléctricas, sistemas financieros y bases de datos gubernamentales. Un ataque cibernético a estas infraestructuras podría paralizar sectores clave de la economía, comprometer información estratégica y debilitar la capacidad de respuesta del Estado ante crisis de seguridad (Comando Conjunto Cibernético de Colombia [C4], 2022).

El alcance de la ciberseguridad en el ámbito militar se ha expandido hacia la consolidación de capacidades de ciberdefensa ofensiva y defensiva. A nivel defensivo, se han implementado estrategias de monitoreo y detección temprana para identificar amenazas cibernéticas antes de que se materialicen. Esto ha permitido a Colombia neutralizar intentos de espionaje y ataques a entidades gubernamentales por parte de actores externos (MDN, 2023). Sin embargo, en el ámbito ofensivo, el país aún enfrenta limitaciones, ya que carece de una doctrina clara sobre el uso de capacidades cibernéticas en operaciones militares activas, algo que otros países han incorporado en sus estrategias de defensa (León, 2021).

Un desafío persistente en el desarrollo de la ciberseguridad en Colombia es la falta de interoperabilidad con la inteligencia militar y las fuerzas especiales. En conflictos modernos, el uso de herramientas cibernéticas no solo permite la defensa de infraestructuras, sino también el apoyo a operaciones ofensivas, como la interrupción de redes de comunicación enemigas o la recopilación de inteligencia a partir del acceso a sistemas de información adversarios (Rodríguez y Garzón, 2024). La ausencia de una doctrina de integración entre la ciberseguridad y las demás capacidades militares limita su efectividad en el contexto de guerra híbrida. Sin embargo, la región carece de mecanismos eficaces de cooperación

interestatal en ciberseguridad, lo que reduce la capacidad de respuesta colectiva ante ataques coordinados (López y Díaz, 2020).

[T2] Inteligencia militar como pilar estratégico

La inteligencia ha sido tradicionalmente el elemento central de la seguridad nacional, permitiendo a los Estados anticiparse a amenazas y tomar decisiones informadas para proteger su soberanía. En Colombia, la inteligencia ha jugado un papel fundamental en el combate contra insurgencias y grupos armados organizados. Sin embargo, en los últimos años, la inteligencia militar ha tenido que expandir su alcance para abordar amenazas emergentes en el ciberespacio, el terrorismo transnacional y los conflictos híbridos (Gómez, 2017).

En el contexto actual, la inteligencia cumple funciones fundamentales en la recolección, análisis e interpretación de información estratégica. A través de la inteligencia humana (HUMINT), inteligencia de señales (SIGINT) y ciberinteligencia, se identifican patrones de amenaza y se desarrollan estrategias para contrarrestarlas antes de que generen impactos significativos en la seguridad nacional (Peña Peña y Olaya Murcia, 2020). En el caso de la inteligencia cibernética, el desafío radica en adaptarse a la rapidez con la que evolucionan las tácticas de ataque en el ciberespacio, donde los grupos criminales pueden operar con gran flexibilidad y anonimato.

Otro aspecto crucial es la contrainteligencia, que tiene como objetivo proteger la información sensible y prevenir la infiltración de agentes hostiles dentro de las estructuras de defensa del país. Colombia ha enfrentado desafíos significativos en esta área, dado que los grupos armados y las organizaciones criminales han desarrollado sofisticadas estrategias de recolección de información que ponen en riesgo la seguridad operativa del Estado (Rodríguez y Garzón, 2024).

inteligencia pierde capacidad de respuesta frente a amenazas dinámicas y en constante evolución. A pesar de los avances doctrinales, la inteligencia estratégica colombiana enfrenta desafíos en su integración tecnológica y operativa (González, 2019). En conflictos modernos, la inteligencia debe servir como un puente entre la ciberseguridad y las unidades operativas en campo, permitiendo que la información recopilada en el ciberespacio sea utilizada para operaciones estratégicas en terreno (León, 2021). Sin esta integración efectiva, la inteligencia pierde capacidad de respuesta frente a amenazas dinámicas y en constante evolución.

[T2] Fuerzas Especiales en la seguridad nacional

Las fuerzas especiales representan la punta de lanza de la capacidad militar colombiana, especializadas en operaciones de alto impacto y misiones en entornos hostiles. Estas unidades están entrenadas para actuar con velocidad, precisión y autonomía táctica, lo que les permite ejecutar operaciones de rescate, combate irregular y neutralización de amenazas estratégicas con un alto grado de efectividad (Montero Moncada, 2020).

Dentro de sus principales funciones, las fuerzas especiales han sido fundamentales en la guerra irregular y en la lucha contra el narcotráfico, insurgencias y grupos armados organizados. Sin embargo, el panorama de amenazas ha cambiado, y estos cuerpos de élite enfrentan el reto de adaptarse a nuevos escenarios de conflicto donde la guerra híbrida y el ciberespacio juegan un papel central (Rodríguez y Garzón, 2024).

El alcance de las fuerzas especiales en la seguridad nacional se extiende más allá de las misiones tradicionales de combate, ya que cada vez es más frecuente la necesidad de operaciones conjuntas con inteligencia y ciberseguridad. La guerra moderna requiere que las unidades de fuerzas especiales sean capaces de utilizar información cibernética en tiempo real, emplear herramientas de guerra electrónica y realizar operaciones coordinadas con el Comando Cibernético y las agencias de inteligencia (Peña Peña y Olaya Murcia, 2020).

No obstante, Colombia aún enfrenta desafíos en la modernización de estas fuerzas para que puedan operar de manera efectiva en un entorno de guerra multidimensional. Sin una integración doctrinal entre las capacidades físicas y digitales, las fuerzas especiales pueden quedar en desventaja frente a adversarios que han adoptado estrategias más flexibles y digitalizadas para el combate. En América Latina, las fuerzas especiales aún deben adaptar sus doctrinas al entorno digital, incorporando herramientas tecnológicas en operaciones en terreno (Chaparro, 2021).

[T1] Integración ciberseguridad, inteligencia, fuerzas especiales en la formulación de estrategias defensa y respuesta ante amenazas.

La evolución del panorama de seguridad ha llevado a que los conflictos modernos se desarrollen en múltiples dimensiones, combinando operaciones físicas y digitales en lo que se conoce como guerra híbrida (Puyosa, 2021). Este tipo de confrontación, caracterizado por la combinación de tácticas convencionales, ciberataques, desinformación y operaciones encubiertas, plantea una amenaza compleja y persistente que exige una respuesta articulada por parte del Estado. En este contexto, la integración de la ciberseguridad, la inteligencia y las fuerzas especiales se ha convertido en un factor determinante para la efectividad de las estrategias de defensa en Colombia. La capacidad de un Estado para proteger su infraestructura crítica, anticipar amenazas y ejecutar operaciones de precisión depende de la articulación efectiva de estos tres pilares estratégicos (Rodríguez y Garzón, 2024).

Cada uno de estos componentes cumple una función complementaria en el diseño y ejecución de respuestas integrales frente a amenazas contemporáneas. La ciberseguridad actúa como la primera línea de defensa en el ámbito digital, garantizando la protección de

infraestructuras críticas y redes de comunicación. La inteligencia, por su parte, ofrece el insumo estratégico necesario para detectar, analizar y anticipar acciones hostiles tanto en el plano físico como en el cibernético. Finalmente, las fuerzas especiales representan la capacidad operativa de respuesta inmediata en escenarios de alta complejidad, con posibilidad de intervención quirúrgica y despliegue en condiciones adversas. No obstante, cuando estas capacidades operan de forma aislada, se limitan entre sí; por el contrario, cuando están integradas bajo una doctrina común, potencian significativamente la eficacia de la defensa nacional.

A nivel internacional, modelos de seguridad como los implementados por Estados Unidos, Reino Unido e Israel han demostrado que la sinergia entre inteligencia, ciberseguridad y fuerzas especiales no solo fortalece la capacidad defensiva, sino que también permite el desarrollo de estrategias ofensivas que neutralizan amenazas en tiempo real (Peña Peña y Olaya Murcia, 2020). Estos casos evidencian que la integración de estas capacidades no es solo una mejora táctica, sino un cambio estructural en la concepción misma del poder militar y la defensa estatal. En Colombia, aunque existen avances en la consolidación de capacidades en cada uno de estos ámbitos, persisten brechas en su integración operativa y doctrinal, lo que limita la respuesta ante amenazas contemporáneas (Montero Moncada, 2020). Este objetivo, por tanto, busca examinar las condiciones necesarias para una integración funcional y estratégica entre estos tres componentes, identificar experiencias exitosas y proponer lineamientos que fortalezcan la capacidad del Estado para responder, de forma coordinada y eficaz, a los desafíos del nuevo entorno de seguridad.

[T2] Articulación de la ciberseguridad en estrategias de defensa

La ciberseguridad es un componente fundamental en la formulación de estrategias de defensa, ya que el ciberespacio se ha convertido en un escenario de conflicto en el que grupos criminales, insurgentes y actores estatales hostiles buscan debilitar la estabilidad del país. En Colombia, la articulación de la ciberseguridad con las demás capacidades estratégicas se ha desarrollado principalmente a través del Comando Conjunto Cibernético (C4), el cual tiene la responsabilidad de coordinar las operaciones de defensa digital del Estado (Ministerio de Defensa Nacional [MDN], 2023).

Uno de los principales desafíos en esta articulación es la integración de la ciberseguridad con la inteligencia militar. La inteligencia cibernética, que se basa en la recolección, monitoreo y análisis de información digital, debe estar alineada con las estrategias de inteligencia tradicional para que los datos recopilados en el ámbito digital sean utilizados en la planificación de misiones operacionales (Comando Conjunto Cibernético de Colombia [C4], 2022). Sin embargo, en el caso colombiano, la falta de interoperabilidad entre estos sistemas ha generado dificultades en la sincronización de información, lo que impide una respuesta rápida y efectiva ante ataques en el ciberespacio.

Otro aspecto clave en la integración de la ciberseguridad en las estrategias de defensa es su vinculación con las operaciones de fuerzas especiales. En los conflictos modernos, las unidades de élite deben operar en entornos donde la guerra electrónica, el acceso a información digital y la disrupción de redes de comunicación enemigas juegan un papel determinante en el éxito de una misión (Rodríguez y Garzón, 2024). No obstante, la doctrina militar colombiana aún no ha desarrollado un modelo de operaciones conjuntas entre unidades de ciberseguridad y fuerzas especiales, lo que limita la capacidad del país para ejecutar misiones ofensivas en el ciberespacio. Potencias como Estados Unidos han integrado

la ciberseguridad en su doctrina militar, estableciendo alianzas entre el sector defensa y la industria tecnológica como parte de su base operativa (Cordesman, 2019).

[T2] El rol de la inteligencia en la integración operativa

La inteligencia es el vínculo central entre la ciberseguridad y las fuerzas especiales, ya que proporciona información estratégica y táctica que permite la formulación de estrategias de defensa y la planificación de misiones operativas (Gómez, 2017). A nivel doctrinal, la inteligencia militar en Colombia ha evolucionado significativamente, ampliando sus capacidades hacia el análisis de datos en tiempo real, la inteligencia de señales (SIGINT) y la inteligencia geoespacial (GEOINT) (León, 2021). Sin embargo, el principal desafío radica en la fusión efectiva de estas capacidades con la ciberseguridad y las fuerzas especiales para potenciar su impacto en la seguridad nacional.

Uno de los ejemplos más relevantes en la integración de la inteligencia en estrategias de defensa es el uso de inteligencia cibernética en operaciones de fuerzas especiales. En países con doctrinas avanzadas, como Estados Unidos e Israel, las unidades de élite dependen en gran medida de datos obtenidos a través del ciberespacio para planificar y ejecutar misiones con precisión quirúrgica (Peña Peña y Olaya Murcia, 2020). En el caso colombiano, esta coordinación aún es incipiente, aunque se han reportado avances en la implementación de tecnologías de vigilancia avanzada y análisis de datos en tiempo real en operaciones contra grupos armados organizados.

En la formulación de estrategias de defensa, la inteligencia también desempeña un papel crucial en la anticipación de amenazas híbridas, como ataques combinados que incluyen ciberataques y acciones físicas simultáneas. Para mejorar su efectividad, Colombia debe desarrollar una doctrina de inteligencia integrada que permita una mayor colaboración entre los analistas de inteligencia, los equipos de ciberseguridad y las unidades operacionales

(Montero Moncada, 2020). Según el Global Cybersecurity Outlook, los ciberataques sofisticados seguirán creciendo, lo que exige una preparación integral y coordinada de los Estados (World Economic Forum, 2023).

[T2] Fuerzas especiales y la integración con ciberseguridad e inteligencia

Las fuerzas especiales han sido históricamente la punta de lanza en la ejecución de misiones de alto valor estratégico. Su entrenamiento y capacidades les permiten operar en entornos de alta complejidad, pero en la era digital, su éxito depende de su capacidad para trabajar en conjunto con la ciberseguridad y la inteligencia (Rodríguez y Garzón, 2024).

En el contexto colombiano, la integración de las fuerzas especiales con estas capacidades se ha evidenciado en operaciones conjuntas donde la inteligencia ha permitido localizar objetivos estratégicos en tiempo real. Sin embargo, en comparación con otros países, Colombia aún no ha desarrollado una doctrina formal en la que las fuerzas especiales utilicen de manera sistemática herramientas de ciberseguridad para mejorar su eficacia operativa (León, 2021).

Uno de los aspectos clave en esta integración es el uso de tecnologías avanzadas para la recopilación y análisis de información en el terreno. En escenarios modernos, las fuerzas especiales deben contar con acceso en tiempo real a datos de inteligencia que les permitan tomar decisiones tácticas con rapidez (Montero Moncada, 2020). Esto implica la necesidad de fortalecer la interoperabilidad entre los sistemas de inteligencia, ciberseguridad y operaciones en campo, garantizando que las unidades de élite cuenten con información precisa y actualizada antes de cada misión.

La articulación entre fuerzas especiales, ciberseguridad e inteligencia también se ha visto reflejada en el uso de operaciones psicológicas y guerra informativa como parte de las estrategias de defensa. La desinformación, la manipulación del discurso público y el control

del flujo de información son elementos que juegan un papel determinante en la guerra híbrida, por lo que Colombia debe desarrollar una doctrina que integre estos elementos en la formulación de sus estrategias de defensa (Puyosa, 2021). La evolución de la guerra moderna ha llevado a que la seguridad cibernética y la guerra convencional se integren como frentes interdependientes (Singer y Friedman, 2014).

[T1] Integración ciberseguridad, inteligencia y fuerzas especiales en formulación de estrategias defensa y respuesta ante amenazas.

[T2] Logros en la integración de ciberseguridad, inteligencia y fuerzas especiales

Colombia ha logrado avances significativos en la coordinación de sus capacidades de ciberseguridad, inteligencia y fuerzas especiales dentro del marco de la seguridad nacional. Uno de los principales logros ha sido la consolidación de una estructura institucional robusta, en la que destacan el Comando Conjunto Cibernético (CCOC), el Centro Cibernético Policial (CCP) y el Equipo de Respuesta a Emergencias Cibernéticas (ColCERT), entidades que han fortalecido la capacidad del Estado para responder a amenazas en el ciberespacio (Ministerio de Defensa Nacional [MDN], 2023). La formulación de la Política Nacional de Seguridad Digital, establecida en el Documento CONPES 3854 de 2016, ha permitido una mayor articulación interinstitucional, estableciendo directrices claras para la protección de infraestructuras críticas y la respuesta a incidentes cibernéticos (Departamento Nacional de Planeación [DNP], 2016).

En el ámbito de la inteligencia y las fuerzas especiales, Colombia ha desarrollado capacidades avanzadas de fusión de inteligencia para el combate a amenazas transnacionales. Operaciones como *Jaque* y *Camaleón* han demostrado la eficacia de una planificación

estratégica conjunta entre unidades de inteligencia y fuerzas especiales, logrando neutralizar objetivos de alto valor y desarticular redes criminales de manera precisa (Montero Moncada, 2020). Además, la adopción de un modelo de guerra preventiva ha permitido fortalecer la colaboración interinstitucional en la identificación de amenazas emergentes, optimizando la capacidad de respuesta del Estado ante escenarios de guerra híbrida (León, 2021). El siguiente esquema representa la integración funcional y doctrinal de las tres capacidades analizadas. Cada componente aporta elementos diferenciados, pero interdependientes, que deben articularse bajo una doctrina operativa común orientada a escenarios de guerra híbrida y defensa anticipativa:

Otro aspecto clave ha sido la cooperación internacional en seguridad y defensa. Colombia ha establecido alianzas estratégicas con actores globales como Estados Unidos, la OTAN y organismos multilaterales como la OEA, lo que ha permitido mejorar el intercambio de información en ciberseguridad e inteligencia militar, así como fortalecer el entrenamiento de fuerzas especiales en operaciones de alto riesgo (Peña Peña y Olaya Murcia, 2020).

[T2] Limitaciones y barreras para una coordinación efectiva

A pesar de estos avances, persisten desafíos significativos en la integración efectiva de estos tres pilares estratégicos. Una de las principales limitaciones es la fragmentación institucional y la falta de interoperabilidad tecnológica. Las plataformas utilizadas por las diferentes agencias de seguridad no siempre son compatibles, lo que dificulta el intercambio oportuno de información y la toma de decisiones en tiempo real (Rodríguez y Garzón, 2024). Este problema se ve agravado por la ausencia de un marco doctrinal único que permita la unificación de procedimientos y protocolos operativos entre ciberseguridad, inteligencia y fuerzas especiales (MDN, 2023).

Otra barrera crítica es la escasez de talento especializado en ciberseguridad y análisis de inteligencia avanzada. Si bien Colombia ha avanzado en la formación de especialistas en estas áreas, la rápida evolución de las amenazas digitales y la sofisticación de los actores no estatales han generado un déficit de profesionales altamente capacitados en tecnologías emergentes y guerra cibernética (León, 2021). Esto afecta la capacidad operativa del Estado para anticipar y contrarrestar ataques cibernéticos sofisticados, así como para optimizar la ejecución de misiones especiales basadas en inteligencia digital (Puyosa, 2021).

Además, el marco legal actual no está completamente adaptado a las dinámicas de las amenazas cibernéticas y la guerra híbrida. Aunque existen esfuerzos para actualizar la normativa de seguridad y defensa, aún persisten vacíos en la regulación de operaciones cibernéticas ofensivas, contrainteligencia digital y uso de inteligencia artificial en la seguridad nacional (DNP, 2023). Esta falta de claridad legal limita la capacidad del Estado para actuar con rapidez ante amenazas transnacionales y ataques coordinados en múltiples dominios (Gómez, 2017). Estas limitaciones reflejan una brecha generalizada en ciberdefensa a nivel regional, donde los marcos legales y operativos aún son débiles (Baylon y Brunt, 2015).

[T2] Retos para fortalecer la interoperabilidad y optimizar el impacto en la seguridad nacional

El fortalecimiento de la coordinación entre ciberseguridad, inteligencia y fuerzas especiales requiere superar una serie de retos estratégicos, entre los que destacan:

Adaptación a amenazas híbridas y de alta tecnología. La guerra contemporánea se caracteriza por la combinación de operaciones físicas y digitales, lo que exige la integración

total de la ciberinteligencia en la planificación y ejecución de misiones especiales. Para ello, es necesario dotar a las unidades de fuerzas especiales de herramientas avanzadas de guerra electrónica, ciberdefensa táctica y análisis de datos en tiempo real (Montero Moncada, 2020).

Actualización del marco estratégico y normativo: Colombia debe acelerar la actualización de su doctrina de seguridad para reflejar la convergencia de dominios y garantizar la protección integral de infraestructuras críticas, el uso legítimo de operaciones cibernéticas ofensivas y la cooperación internacional en ciberseguridad (MDN, 2023). Esto implica la armonización de la legislación colombiana con estándares internacionales, como el Convenio de Budapest sobre ciberdelincuencia y las directrices de la OTAN en ciberoperaciones (DNP, 2023).

1. **Fortalecimiento de la comunidad de inteligencia y la confianza interinstitucional**: La efectividad del tridente estratégico depende de la creación de **centros de fusión de inteligencia**, donde analistas cibernéticos, especialistas en inteligencia estratégica y unidades operativas trabajen de manera coordinada (Peña Peña y Olaya Murcia, 2020). Para ello, es fundamental **reducir la compartimentación excesiva de información** y fomentar la **colaboración permanente entre actores clave del sector defensa y seguridad** (Rodríguez y Garzón, 2024).
2. **Cooperación internacional en ciberseguridad e inteligencia**: Dado que muchas amenazas en el ciberespacio son de **naturaleza transnacional**, Colombia debe fortalecer su cooperación con socios estratégicos para intercambiar inteligencia sobre ataques cibernéticos, amenazas híbridas y redes criminales transnacionales (León, 2021). Esto permitirá **fortalecer la respuesta del país ante ciberataques dirigidos**

contra infraestructuras críticas y mejorar la interoperabilidad con fuerzas militares aliadas (Puyosa, 2021).

La integración de la ciberseguridad, la inteligencia y las fuerzas especiales es un pilar esencial para la seguridad y defensa de Colombia en el siglo XXI. Si bien el país ha logrado avances significativos en la creación de estructuras de seguridad digital, el fortalecimiento de la inteligencia estratégica y la modernización de sus fuerzas especiales aún enfrenta desafíos importantes en términos de interoperabilidad, talento especializado y actualización normativa.

Para superar estos desafíos, se recomienda desarrollar una estrategia de seguridad nacional basada en una doctrina conjunta, fortalecer la colaboración interinstitucional, invertir en la capacitación continua del talento humano y promover la cooperación internacional en ciberseguridad e inteligencia. Solo a través de una visión integrada y adaptada a las amenazas modernas, Colombia podrá consolidar su capacidad para enfrentar los desafíos emergentes y fortalecer su posición en el escenario global de la seguridad y defensa. La integración de capacidades cibernéticas no puede ser un apéndice, sino un eje estratégico dentro de las políticas de defensa regional (Brito y Casanova, 2022).

A partir del análisis documental y comparativo desarrollado, se consolidaron hallazgos clave organizados en torno a las categorías analíticas centrales del estudio: ciberseguridad, inteligencia militar, fuerzas especiales e integración estratégica. Esta síntesis metodológica permite identificar avances, brechas y potencialidades dentro del aparato de defensa nacional colombiano:

- **Ciberseguridad:** Colombia ha avanzado significativamente con la creación del Comando Conjunto Cibernético (C4) y ColCERT, así como con la formulación de políticas públicas como el CONPES 3854 de 2016. No obstante, aún persiste una

débil articulación con los entornos operativos, especialmente en lo relacionado con capacidades ofensivas, interoperabilidad con fuerzas especiales y recolección de inteligencia táctica en el ciberespacio (Ministerio de Defensa Nacional, 2023; León, 2021).

- **Inteligencia militar:** La doctrina de inteligencia ha transitado desde un enfoque reactivo hacia modelos más preventivos, apoyados en SIGINT, GEOINT y análisis predictivo. Sin embargo, las capacidades de integración con ciberinteligencia y despliegue operativo aún presentan vacíos estructurales (Gómez, 2017; González, 2019). La falta de interoperabilidad entre plataformas y la compartimentación de la información afectan la eficacia estratégica.
- **Fuerzas especiales:** Se ha consolidado su capacidad táctica en entornos rurales y asimétricos, siendo clave en operaciones como Jaque y Camaleón. A pesar de ello, se identifican debilidades en la adopción de herramientas digitales, acceso a inteligencia cibernética en tiempo real y en la doctrina conjunta con capacidades tecnológicas (Rodríguez & Garzón, 2024; Montero Moncada, 2020).
- **Integración estratégica:** Aunque existen experiencias puntuales de cooperación interinstitucional, aún no se cuenta con un marco doctrinal sólido que articule las tres capacidades bajo una lógica operativa común. La ausencia de centros de fusión de inteligencia ciber-operacional, marcos legales actualizados y protocolos de interoperabilidad impide consolidar el tridente estratégico de forma estructural (Peña Peña & Olaya Murcia, 2020; DNP, 2023).

[T2] Propuesta operativa para la implementación del "Tridente Estratégico"

Con el fin de materializar la integración de ciberseguridad, inteligencia y fuerzas especiales como eje de la defensa nacional, se propone un plan estructurado en cinco fases operativas.

Este modelo busca garantizar que la estrategia pase de un nivel doctrinal a un nivel aplicable en el terreno, con responsabilidades claras, recursos definidos e indicadores de éxito.

La propuesta del "Tridente Estratégico" se ilustra a través de un esquema triangular en el que cada vértice representa una capacidad estratégica: ciberseguridad, inteligencia militar y fuerzas especiales. El centro del triángulo simboliza la integración doctrinal y operativa, que permite articular las tres capacidades para una defensa nacional anticipativa y coordinada. Las flechas bidireccionales representan la interoperabilidad y el flujo constante de información y recursos entre cada pilar.

Tabla 2

Propuesta por fases

Fase	Objetivo	Actividades clave	Responsable principal	Recursos necesarios	Indicadores de éxito
Diagnóstico	Identificar brechas y capacidades actuales en los tres componentes	Auditoría de capacidades, mapeo de procesos, inventario tecnológico	Ministerio de Defensa Nacional – C4 – Dirección de Inteligencia	Equipos técnicos, consultores especializados, acceso a información clasificada	Informe diagnóstico aprobado por el Consejo de Seguridad Nacional
Diseño doctrinal	Establecer un marco unificado de operación e interoperabilidad	Redacción de doctrina integrada, protocolos conjuntos, definición de estándares de interoperabilidad	Dirección de Inteligencia Militar – Jefatura de Operaciones Especiales	Grupo doctrinal, asesores jurídicos y operativos	Documento doctrinal adoptado mediante resolución ministerial
Capacitación y alistamiento	Preparar al personal en competencias conjuntas	Programas de formación en ciberdefensa táctica, manejo de inteligencia en tiempo real, coordinación de operaciones especiales	Escuela de Guerra – Centro de Entrenamiento de Fuerzas Especiales	Plataformas de simulación, instructores nacionales e internacionales	% de personal certificado en las tres capacidades
Implementación	Desplegar operaciones conjuntas bajo el modelo tridente	Ejecución de misiones integradas, pruebas piloto en operaciones de alto valor, ejercicios conjuntos nacionales e internacionales	Comandos conjuntos regionales – C4 – Dirección de Inteligencia	Recursos de despliegue, sistemas de comunicación interoperables	Tiempo de respuesta < 15 min en incidentes críticos
Evaluación y mejora continua	Medir impacto y optimizar el modelo	Auditorías operativas, revisión de indicadores, retroalimentación y actualización doctrinal	Inspectoría General – Centro de Estudios Estratégicos	Sistemas de análisis de datos, evaluadores externos	Informe anual de desempeño con mejoras implementadas

Fuente: Elaboración propia acorde a analisis

[T1] Conclusiones

El análisis de las funciones, alcances y particularidades de la ciberseguridad, la inteligencia militar y las fuerzas especiales en el contexto colombiano permitió comprender que, si bien cada una de estas capacidades ha experimentado avances relevantes en términos normativos, técnicos y operativos, aún se encuentran operando de forma relativamente independiente. La ciberseguridad, reconocida como una prioridad estratégica, ha sido institucionalizada mediante políticas como el CONPES 3854 y la creación del Comando Conjunto Cibernético (C4), lo que demuestra el compromiso del Estado con la protección del ciberespacio.

Por su parte, la inteligencia militar ha evolucionado desde un enfoque reactivo hacia uno más preventivo, adaptándose progresivamente a las amenazas del entorno digital. Las fuerzas especiales, tradicionalmente eficaces en escenarios de combate asimétrico, han consolidado su rol en operaciones de alto valor estratégico, aunque con limitaciones evidentes para operar en dominios virtuales. Esta revisión evidencia que, aunque se han consolidado capacidades individuales robustas, la falta de una visión común y una articulación doctrinal limita el aprovechamiento del potencial conjunto que ofrecen estas tres áreas para la seguridad nacional.

En relación con la integración operativa y doctrinal de las capacidades de ciberseguridad, inteligencia y fuerzas especiales en las estrategias de defensa nacional, los hallazgos de esta investigación reflejan que Colombia se encuentra en una fase intermedia de desarrollo. Si bien se han dado pasos importantes en la construcción de capacidades sectoriales y se han emprendido acciones puntuales de cooperación interagencial, aún no se ha logrado consolidar un modelo integral de planeación conjunta que incorpore estas áreas como componentes interdependientes de una misma estrategia nacional de defensa. A nivel internacional, modelos como los implementados por Estados Unidos, Israel y los países de

la OTAN demuestran que la integración de estas capacidades no solo mejora la capacidad de respuesta ante amenazas híbridas, sino que permite una proyección estratégica ofensiva basada en anticipación, precisión y velocidad. La ausencia de esta sinergia en el contexto colombiano se traduce en brechas de interoperabilidad, fragmentación del flujo de inteligencia y limitaciones para ejecutar operaciones conjuntas efectivas en tiempo real. Por tanto, el país debe avanzar en la formulación de un marco doctrinal y normativo unificado que promueva la coordinación desde la fase de planeación hasta la ejecución táctica de operaciones.

Colombia ha alcanzado logros importantes en el fortalecimiento de sus capacidades de defensa digital y en la profesionalización de sus fuerzas armadas, especialmente en lo relacionado con ciberseguridad e inteligencia estratégica. La creación del ColCERT, la actualización de la Estrategia Nacional de Ciberseguridad y los ejercicios conjuntos entre unidades de inteligencia y fuerzas especiales han permitido aumentar el nivel de preparación institucional ante amenazas complejas. Sin embargo, estos avances aún coexisten con limitaciones estructurales que obstaculizan la consolidación de un sistema de defensa plenamente integrado. Entre estas limitaciones se destacan la fragmentación institucional, la escasa interoperabilidad tecnológica entre agencias, la duplicación de funciones, la insuficiencia de personal especializado en ciberdefensa y la falta de adaptación del marco legal a las nuevas realidades del conflicto híbrido. A ello se suma la limitada cooperación internacional efectiva en áreas clave como inteligencia técnica y guerra electrónica. Para superar estos desafíos, se requiere un esfuerzo sostenido y coordinado entre los distintos actores del sector defensa y seguridad, que incluya inversión en talento humano, actualización doctrinal, interoperabilidad de sistemas y fortalecimiento de alianzas regionales y globales.

La presente investigación demuestra que la integración efectiva de ciberseguridad, inteligencia y fuerzas especiales en el marco de una doctrina del "tridente estratégico" constituye una necesidad imperativa para la defensa nacional de Colombia en el contexto contemporáneo.

Las amenazas actuales —caracterizadas por su naturaleza híbrida, transnacional, asimétrica y digital— exigen una capacidad de respuesta flexible, anticipada y coordinada que solo puede alcanzarse mediante la sinergia de estas tres capacidades. No se trata únicamente de sumar recursos o funciones, sino de transformar el modelo de pensamiento estratégico hacia una visión convergente que integre el poder de las tecnologías digitales con la precisión operativa de las fuerzas especiales y la capacidad analítica de la inteligencia militar. Alcanzar este objetivo requiere la construcción de una doctrina nacional que promueva la interoperabilidad desde el diseño institucional, así como una cultura organizacional orientada a la cooperación interagencial y la adaptación continua. Solo así, Colombia podrá garantizar una defensa efectiva de su soberanía, proteger sus activos estratégicos y posicionarse como un actor con capacidad de disuasión y respuesta en el escenario global de la seguridad y defensa del siglo XXI.

Referencias

Baylon, C., & Brunt, R. (2015). *Cybersecurity in Latin America: Threats, trends and policy responses*. Oxford Internet Institute. https://doi.org/10.2139/ssrn.2614540

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brito, L., & Casanova, M. (2022). Ciberdefensa como componente estratégico en la seguridad regional sudamericana. *Revista de Estudios Estratégicos, 15*(2), 79–101. https://doi.org/10.5354/0719-1529.2022.66268

Cáceres García, J. A. (2017). Colombia, estrategia nacional en ciberseguridad y ciberdefensa. *Air & Space Power Journal en Español, 29*(1), 86–93.

Chaparro, S. (2021). *Las Fuerzas Especiales en América Latina: doctrinas, roles y desafíos*. FLACSO Ecuador.

Comando Conjunto Cibernético de Colombia (C4). (2022). *Informe de capacidades y amenazas digitales en Colombia*. Ministerio de Defensa Nacional.

Cordesman, A. H. (2019). *Cybersecurity and the defense industrial base*. Center for Strategic and International Studies. https://www.csis.org

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.

Departamento Nacional de Planeación (DNP). (2016). *CONPES 3854: Política Nacional de Seguridad Digital*. Gobierno de Colombia. https://colaboracion.dnp.gov.co

Departamento Nacional de Planeación (DNP). (2023). *Estrategia Nacional de Ciberseguridad y Defensa Digital*. Gobierno de Colombia.

Flick, U. (2018). *An introduction to qualitative research* (6th ed.). SAGE.

Gómez, J. D. (2017). La inteligencia militar y su evolución en Colombia. *Revista ACORE, (194)*, 22–25.

González, J. F. (2019). Inteligencia estratégica en Colombia: Evolución y desafíos. *Revista Criminalidad, 61*(2), 103–122. https://revistas.policia.edu.co/index.php/criminalidad/article/view/1186

Le Billon, P., Roa-García, M. C., & López-Granada, A. R. (2020). Territorial peace and gold mining in Colombia: Local peacebuilding, bottom-up development and the defence of territories. *Conflict, Security & Development, 20*(3), 303–333. https://doi.org/10.1080/14678802.2020.1763820

León, F. (2021). *Evolución de la inteligencia militar en Colombia: Desafíos y oportunidades*. Escuela Superior de Guerra.

López, C., & Díaz, M. (2020). Ciberseguridad y cooperación internacional en América Latina. *Revista CS, (30)*, 25–48. https://doi.org/10.18046/recs.i30.4003

Ministerio de Defensa Nacional (MDN). (2023). *Estrategia Nacional de Ciberseguridad y Ciberdefensa en Colombia*. Gobierno de Colombia. https://www.mindefensa.gov.co

Montero Moncada, L. A. (2020). *El tridente del poder estratégico: Inteligencia, operaciones especiales y poder ciber en el siglo XXI*. Escuela Superior de Guerra.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). *Strategic integration of cyber capabilities in military planning*. https://ccdcoe.org

Peña Peña, W., & Olaya Murcia, M. (2020). El tridente estratégico y las capacidades del Ejército Nacional de Colombia. En L. A. Montero Moncada (Ed.), *El tridente del poder estratégico: Inteligencia, operaciones especiales y poder ciber en el siglo XXI* (pp. 195–213). Escuela Superior de Guerra.

Puyosa, I. (2021). *Ciberseguridad y guerra híbrida en América Latina*. Editorial Universitaria.

Rodríguez, J. N., & Garzón, O. (2024). Amenazas cibernéticas contemporáneas: Retos y desafíos para las operaciones especiales en Colombia. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 93–114). Sello Editorial ESDEG.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

United Nations Office on Drugs and Crime (UNODC). (2022). *Cybercrime in Latin America and the Caribbean: Regional assessment*. https://www.unodc.org/documents/cybercrime/Cybercrime-LAC-Report-2022.pdf

Waltz, K. (2000) Teoría de la Política Internacional. Buenos Aires.

Walt, S. (1998) One world, many theories, Foreign Policy.

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023