Revisión sistemática de los fundamentos doctrinales, pedagógicos y tecnológicos para la inclusión de la guerra cibernética como asignatura en la doctrina militar de Colombia.

Derwin Libardo Martínez Rodríguez

Asesor

Jhon Manuel Soto Cala

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería de Sistemas

2026

Nota de Aceptación

Firma Director(a) Trabajo de grado

Firma presidente del Jurado

Firma Jurado

Dedicatoria

Con profunda gratitud y humildad, dedico este trabajo de opción de grado, fruto de un arduo esfuerzo y dedicación, a quienes han sido mi soporte y mi inspiración constante. En primer lugar, a Dios, por iluminar mi camino, por la salud y la sabiduría que me han permitido alcanzar esta meta tan anhelada. A mis amados padres, por su amor incondicional, su sacrificio y su incansable apoyo. Sus enseñanzas y valores han sido el cimiento de mi vida y la fuerza motriz para superar cada desafío. A mi querido hermano, por su compañía, su aliento y por compartir conmigo la alegría de cada paso en este camino. Su presencia ha sido un motor invaluable. A mi maravillosa esposa, por su amor inquebrantable, su entendimiento y su paciencia sin límites. Te agradezco por ser mi compañera de vida, por tu apoyo sin condiciones en los tiempos difíciles y por festejar conmigo cada pequeño progreso; tu fe en mí ha sido esencial. A mi adorado hijo, el mayor tesoro y la razón de mi perseverancia, espero que este logro sea un faro y una muestra de que los sueños se vuelven realidad con dedicación y esfuerzo; eres mi principal motivación.

Finalmente, a la Universidad Nacional Abierta y a Distancia (UNAD), por ofrecerme la posibilidad de capacitarme, de desarrollarme en el ámbito profesional y de finalizar este período académico. Estoy agradecido con la plataforma y el saber que me facilitaron un tema de vital importancia como lo es "La incorporación de la guerra cibernética en la doctrina militar colombiana", contribuyendo así al análisis de un campo tan relevante para la defensa y seguridad de nuestro país.

Este trabajo es para todos ustedes, con todo mi amor y gratitud.

Resumen

La finalidad de este trabajo de grado es analizar la importancia y los fundamentos para incluir la guerra cibernética como una asignatura, materia o tema central en el plan de estudio de la doctrina militar colombiana, en concordancia con estrategias pedagógicas que verifiquen competencias doctrinales y digitales relacionadas con guerra cibernética. Esto resulta fundamental hoy en día para robustecer la educación militar en Colombia (Rivera Alturo, L. M., & Hernández García, S. A., 2023). Para ello se realiza una revisión sistemática, empleando la metodología PRISMA 2020, para establecer una propuesta de currículo que respalde la inclusión de la asignatura de guerra cibernética en la doctrina militar colombiana. Esta revisión abarca las evidencias publicadas entre los años 2020 y 2025 sobre la guerra cibernética y su impacto en la doctrina militar. En este orden de ideas, "Ciberdefensa y Guerra Cibernética" se convierte en un componente de suma importancia para el currículo militar, cuyo objetivo es que el personal sea capacitado de manera integral en los niveles técnico, profesional y especializado (Díaz, M. E., 2019). La propuesta curricular incluye el uso de herramientas tecnológicas modernas, tales como simulaciones, plataformas digitales que generan una sensación de presencia y realismo, laboratorios virtuales y ejercicios prácticos de defensa y ciberataque. Estos instrumentos ayudan a que los estudiantes interactúen con situaciones digitales hipotéticas o reales de conflicto. Estos métodos promueven la experiencia práctica, apoyan el aprendizaje significativo y fomentan el desarrollo del razonamiento estratégico frente a las recientes amenazas cibernéticas. (Peña Suárez, 2023; Moreno Rodríguez, 2024). Por lo tanto, la asignatura contribuirá significativamente a fortalecer la doctrina militar del país, promoviendo una cultura institucional de renovación tecnológica y de autoridad. Asimismo, la actualización permanente de los integrantes del Ejército Nacional se fomentará como parte de una estrategia integral de

ciberdefensa que enfrenta los desafíos que plantean las tecnologías disruptivas. (Díaz, M. E., 2019; ESDEG, s. f.).

Palabras clave: Asignatura de guerra cibernética, Doctrina militar, Ciberdefensa, PRISMA 2020, Revisión Sistemática.

Abstract

The purpose of this thesis is to analyze the importance and rationale for including cyber warfare as a core subject or theme in the Colombian military doctrine curriculum, in accordance with pedagogical strategies that verify doctrinal and digital competencies related to cyber warfare. The topic is fundamental today for strengthening military education in Colombia (Rivera Alturo, L. M., & Hernández García, S. A., 2023). To this end, a systematic review is conducted, using the PRISMA 2020 methodology, to establish a curriculum proposal that supports the inclusion of cyber warfare as a subject in Colombian military doctrine. This review encompasses evidence published between 2020 and 2025 on cyber warfare and its impact on military doctrine. In this line of thought, "Cyber Defense and Cyber Warfare" becomes a component of utmost importance for the military curriculum, whose objective is that personnel be trained in a comprehensive manner at the technical, professional, and specialized levels (Díaz, M. E., 2019). The curriculum uses modern technology like simulations, digital platforms that feel real, virtual labs, and hands-on exercises for cyber defence and attacks. These tools help students interact with hypothetical or real digital conflict situations. These methods promote hands-on experience, support meaningful learning, and foster the development of strategic reasoning in the face of recent cyber threats. (Peña Suárez, 2022; Moreno Rodríguez, 2024). Therefore, the subject will significantly contribute to strengthening the country's military doctrine, promoting an institutional culture of technological and authority renewal. Likewise, the ongoing professional development of members of the National Army will be encouraged as part of a comprehensive cyberdefense strategy that addresses the challenges posed by disruptive technologies. (Díaz, M. E., 2019; ESDEG, n.d.).

Keywords: Cyber warfare subject, military doctrine, cyber defense, PRISMA 2020, systematic review.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

El propósito de esta monografía es estudiar, con base en la literatura doctrinal y académica publicada entre los años 2020 y 2025, la relevancia y los fundamentos para incluir la guerra cibernética como una asignatura o materia parte del currículo específico en la doctrina militar colombiana.

En el campo de la defensa y seguridad contemporáneas, la guerra cibernética se ha afianzado como uno de los retos doctrinales y estratégicos más relevantes por eso debe formularse como una asignatura. El uso cada vez mayor de tecnologías digitales en las operaciones militares y la ampliación de amenazas cibernéticas han forzado a los países a reconsiderar sus estructuras doctrinales, sus habilidades para responder y sus tácticas para defenderse a nivel nacional (Lindsay, J., Ming Cheung, T., & Reveron, D., 2015). Colombia, en este marco, no ha sido indiferente a los peligros que surgen del ciberespacio. Por eso se hace necesario reforzar su doctrina militar para hacer frente a las ofensivas digitales, las operaciones de desinformación y los conflictos híbridos que mezclan tácticas tradicionales con ataques virtuales (Ministerio de Defensa Nacional, 2022).

El sistema de formación militar de Colombia se encuentra en un período de transformación tanto doctrinal como educativa, en el que la guerra cibernética surge como un área crucial para reforzar las capacidades operativas y estratégicas. En estas condiciones, se ha incluido en el currículo militar nacional una materia o asignatura llamada "Guerra cibernética y ciberdefensa" debido a la necesidad de integrar prácticas académicas y tecnológicas emergentes que faciliten un entendimiento más detallado del ciberespacio como área de riesgo, innovación y conflicto (Peña Suárez, 2023; Gaitán Rodríguez, 2022).

La guerra cibernética, así como otras tecnologías relacionadas, requiere que se apliquen métodos de aprendizaje activo que propicien la inmersión digital a través de simulaciones, ejercicios prácticos de ataque y defensa en contextos controlados, laboratorios virtuales y contenidos interactivos. Estos cursos de acción permiten que los miembros del Ejército Nacional adquieran no solo conocimientos teóricos, sino también habilidades prácticas para encarar riesgos específicos en el ámbito cibernético, superando así las limitaciones de la educación tradicional (Rivera Alturo, L. M., & Hernández García, S. A., 2023).

Además, para asegurar una formación equilibrada en las instituciones militares, es crucial que estos recursos didácticos tecnológicos sean accesibles. La materia sugerida debe ser creada para que todos los alumnos, sin importar su área de especialización o su localización geográfica, puedan acceder a simuladores, plataformas de aprendizaje colaborativo, recursos digitales actualizados y herramientas que promuevan la solución de problemas reales en ambientes digitales. Esto anima a un aprendizaje distinguido, ya que facilita la aplicación de conceptos en contextos operativos ficticios que simbolizan las dinámicas del ciberespacio (Peña Suárez, 2023).

Finalmente, la incorporación de la guerra cibernética como asignatura o materia contribuye a actualizar las doctrinas y a continuar con la formación del personal militar. Fomenta la creación de una cultura institucional centrada en la innovación y la autoridad tecnológica. Así pues, la actualización del currículo no abarca únicamente conocimientos técnicos, sino también valores estratégicos que son esenciales para salvar a la nación ante amenazas digitales complejas. (Peña Suárez, 2023).

Justificación

Para garantizar la defensa y seguridad de Colombia en la era digital, es fundamental incorporar la asignatura de guerra cibernética a la doctrina y formación militar colombiana como una medida tanto educativa como estratégica. Esta investigación justifica francamente la elección de una revisión sistemática (PRISMA 2020) como parte de la metodología, la cual permite identificar, evaluar y sintetizar de forma reproducible la evidencia disponible entre el año (2020–2025), con el fin de detectar vacíos empíricos y doctrinales, y así, garantizar que la propuesta curricular esté sustentada en hallazgos verificables y de calidad (evaluados con CASP). Esto tiene como objetivo que las Fuerzas Militares desarrollen capacidades tecnológicas, cognitivas y doctrinales para anticipar, impedir y contrarrestar de manera integral los ciberataques en un escenario virtual (Gaitán Rodríguez, 2022).

Los procesos de formación militar necesitan una reestructuración continua que implemente métodos pedagógicos alcanzables para todos los miembros, sin importar el contexto religioso o sociopolítico, con la finalidad de garantizar una educación militar de alta calidad, acorde con los principios institucionales y los compromisos en seguridad digital a nivel nacional. La (O.N.U., 2015) Organización de las Naciones Unidas promueve los Objetivos de Desarrollo Sostenible (ODS) como marco para erradicar la desigualdad y fortalecer la justicia social; en el ámbito militar, estos objetivos encuentran eco al promover una doctrina formativa que integre capacidades de ciberdefensa para proteger el Estado frente a amenazas emergentes (Peña Suárez, 2023; Gamboa, J. A., 2023).

Desde una perspectiva educativa, esta inclusión se basa en que es necesario poner al día los procedimientos de enseñanza y aprendizaje en las escuelas de formación militar, incorporando temas relacionados con ciberdefensa, inteligencia digital, evaluación de riesgos,

administración de incidentes y acciones cibernéticas, acorde a las exigencias del contexto mundial (Peña Suárez, 2023). Además, la capacitación o formación en guerra cibernética podría ayudar a consolidar el pensamiento estratégico en los líderes militares del futuro, promoviendo que las decisiones se tomen con conocimiento y ética dentro de las directrices nacionales de defensa y del Derecho Internacional Humanitario.

Además, una educación militar de calidad superior debe estar reducidamente vinculada con los avances tecnológicos significativos, cumpliendo procesos de aprendizaje que incluyan prácticas, simulaciones, laboratorios virtuales y situaciones de amenazas cibernéticas; de esta manera, se conseguirá la vinculación y una interacción efectiva. Este estudio tiene como objetivo evaluar, en términos de referencia, las ventajas pedagógicas de incluir la asignatura de guerra cibernética en las mallas curriculares militares con el fin de lograr la cobertura educativa, reducir las diferencias en habilidades doctrinales y digitales, fortalecer la preparación institucional frente a los retos del ciberespacio (Rivera Alturo, L. M., & Hernández García, S. A., 2023); “Proyecto de formación de oficiales”, 2024).

Según la bibliografía que se ha revisado, (Realpe Díaz, 2019) sostiene que la ciberdefensa no debe considerarse como un componente extra de la doctrina militar, sino como un elemento fundamental que tiene que formar parte del entrenamiento de los oficiales y suboficiales con el fin de garantizar la soberanía digital nacional. Por lo tanto, la formación militar se convierte en un ámbito de cambio donde confluyen la ética institucional, la estrategia y la tecnología.

Simultáneamente, se sugiere examinar el impacto cognitivo del currículo actualizado, estableciendo hasta qué punto la inclusión de la asignatura de guerra cibernética ayuda a

desarrollar habilidades estratégicas, críticas y operativas. Esto se tratará a través de la revisión de documentos y el análisis de referentes doctrinales y académicos, con el objetivo de establecer argumentos fundamentados en pruebas empíricas y apoyados por autores nacionales expertos en educación militar y ciberseguridad (Peña Suárez, 2023; Camacho, J. D., 2016).

Además, es relevante señalar que las tecnologías vinculadas al dominio cibernético se han considerado históricamente como caras o inalcanzables debido a la necesidad de una infraestructura especializada. No obstante, estos desafíos deben analizarse frente a las oportunidades que brindan para desarrollar habilidades militares actuales, tales como la ética cibernética, la resiliencia digital y la toma de decisiones en contextos híbridos de conflicto (Barrero, J. C., 2025) - Política de Educación para la Fuerza Pública 2021-2026, 2022.

Con el fin de construir una doctrina militar moderna y justa, esta investigación se articula en tres ejes fundamentales: educación militar, tecnología aplicada al dominio cibernético y accesibilidad formativa. La sinergia de estos ejes permitirá contribuir a la formación de fuerzas militares con capacidades robustas, equitativas y capaces de enfrentar amenazas tecnológicas, aportando así a la seguridad nacional, la soberanía digital y la justicia institucional.

Finalmente, esta propuesta tiene como objetivo, desde la perspectiva pedagógica-doctrinal, no solo educar a expertos técnicos en defensa cibernética, sino también formar a militares que sean conscientes de las dimensiones estratégicas y éticas del ciberespacio y que estén en condiciones de liderar el proceso de transformación digital de las Fuerzas Armadas. Por lo tanto, se contribuye al cumplimiento de los Objetivos de Desarrollo Sostenible relacionados con la educación de calidad y con la justicia, la paz e instituciones firmes (O.N.U., 2015),

asegurando una formación militar que sea actual, significativa y esté comprometida con la seguridad del país.

A pesar de que Colombia ha avanzado en la creación de unidades de ciberdefensa, sigue existiendo una falta de marcos curriculares integrales, poca coordinación con regulaciones internacionales como el Manual de Tallin (Pessino, 2017) y escasa interoperabilidad a nivel tecnológico. (Fortinet et al., 2024) reporta que, en 2023, el 87% de las organizaciones a nivel global sufrieron por lo menos un error de seguridad y que el 53% notificaron pérdidas superiores al millón de dólares. Esto evidencia cuán apremiante es que la doctrina militar colombiana responda a estas tendencias.

Tabla 1

Brecha de Competencias en Ciberseguridad

Indicador	Valor	Fuente
% de organizaciones con una o más brechas	87%	Fortinet et al., (2024)
% con pérdidas > USD 1M	53%	Fortinet et al., (2024)

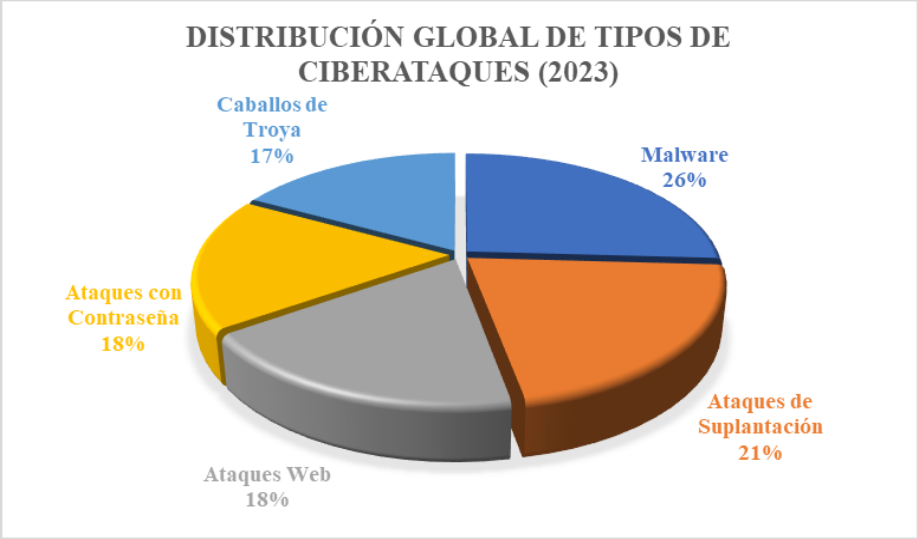
Nota. Informe sobre la brecha de competencias en ciberseguridad indica que las juntas directivas se interesan más en la ciberseguridad. Adaptada de *"Las violaciones consumen tiempo y dinero valioso"* [Texto] (Fortinet et al., 2024), https://www.fortinet.com/content/dam/fortinet/assets/reports/es_la/2024-cybersecurity-skills-gap-report.pdf

Distribución Global de Tipos de Ataques

De acuerdo con el informe de Fortinet et al., (2024) los ataques de phishing, malware y web constituyen aproximadamente el 80 % del total mundial.

Figura 1

Distribución Global de Tipos de Ataques.



Nota. Los cinco principales ataques experimentados con más frecuencia en 2023. Adaptada de *"Un panorama de amenazas conocido"* [Imagen] (Fortinet et al., 2024), https://www.fortinet.com/content/dam/fortinet/assets/reports/es_la/2024-cybersecurity-skills-gap-report.pdf

Contexto Académico

Desde el punto de vista académico, la investigación contribuye a fortalecer el conocimiento científico sobre la relación entre la doctrina militar y la asignatura relacionada con la guerra cibernética, un campo que, pese a que cada vez es más relevante, aún presenta una escasez de estudios sistemáticos en América Latina (Revista Ciberespacio, Tecnología e Innovación, 2024). Esta monografía, además, proporcionará una base conceptual sólida para estudios interdisciplinarios futuros que traten temas como la transformación doctrinal, la ciberseguridad en el ámbito militar y la resiliencia digital.

Asimismo, al proporcionar insumos que pueden ser empleados en los programas académicos del Ejército Nacional y de la UNAD, el estudio adquiere un valor pedagógico. Esto contribuye a potenciar las competencias de análisis e investigación de aquellos que se están formando para ser ingenieros en sistemas o científicos militares.

Contexto Doctrinal

La investigación se centra en las doctrinas, con el objetivo de que los principios sean más adecuados para el entorno militar y estén actualizados con el espacio cibernético. Según el (Ministerio de Defensa Nacional, 2022), aunque la doctrina Damasco acepta las múltiples dimensiones del conflicto, es crucial integrar más a fondo el sistema cibernético en sus directrices operativas y estratégicas (Centro de Doctrina del Ejército, 2020). La investigación mostrará que la guerra cibernética ha cambiado los conceptos tradicionales de defensa, seguridad y soberanía. Esto muestra que es esencial formarse en operaciones de múltiples campos, defensa cibernética ofensiva e inteligencia digital (Arquilla, J., & Ronfeldt, D., 2007). Simultáneamente,

el análisis literario viabilizará manifestar las concordancias y tensiones doctrinales entre autores, puntos de vista internacionales e instituciones. Esto favorecerá la creación de una doctrina militar en Colombia que esté alineada con las amenazas híbridas contemporáneas (Realpe Diaz, M. E., & Cano Martínez, J. J., 2020).

Contexto Práctico

En términos prácticos, el estudio afecta directamente la capacitación técnica y profesional de los ingenieros de sistemas del Ejército Nacional, que desempeñan un papel crucial en la defensa del ciberespacio. El estudio posibilitará la formulación de directrices curriculares específicas que combinen las competencias, los conocimientos y las habilidades requeridas por la guerra cibernética con principios doctrinales, estratégicos y éticos, al determinar cuáles son dichas capacidades. Esto ayudará a desarrollar un perfil profesional más integral, con la capacidad de planificar, ejecutar y evaluar operaciones de defensa digital desde un enfoque soberano e institucional. Igualmente, los resultados de la investigación pueden ser utilizados para tomar decisiones dentro de la institución, planificar la educación y actualizar la doctrina, lo que ayudará a mejorar las capacidades de respuesta y resiliencia frente a incidentes cibernéticos significativos (Centro Cibernético Policial, 2024).

Contexto Social y Estratégico

Esta investigación es relevante desde el punto de vista social y estratégico, ya que la seguridad digital es actualmente un elemento fundamental del bienestar colectivo y de la seguridad humana. Los ataques cibernéticos a infraestructuras vitales tienen el potencial de

impactar las comunicaciones, la energía, el transporte y los servicios públicos fundamentales, lo que tiene un efecto directo en la vida diaria de la ciudadanía (Foro Económico Mundial, 2024). Así pues, es fundamental robustecer la doctrina militar y la formación en ciberdefensa para salvar la soberanía del país, asegurar el desempeño de los servicios indispensables y elevar la confianza pública en las entidades estatales. Finalmente, la investigación promueve el desarrollo de políticas públicas y estrategias educativas que estén alineadas con los objetivos de la Política Nacional de Ciberdefensa y Ciberseguridad 2022-2030. De esta manera, se promueve una cultura digital resiliente y sostenible (Ministerio de Defensa Nacional, 2022).

El impacto de esta investigación es doble: institucional y social. El estudio, en el plano institucional, ayuda a robustecer la Doctrina Damasco y a consolidar la habilidad de ciberdefensa del Ejército Nacional, en una situación donde las amenazas digitales sobrepasan la rapidez de reacción doctrinal. La protección de infraestructuras críticas en áreas como la salud, las finanzas, la energía y las comunicaciones asegura que los servicios fundamentales para la ciudadanía civil continúen.

De acuerdo con el (Foro Económico Mundial, 2024), los riesgos cibernéticos constituyen una de las cinco amenazas más relevantes para la estabilidad de las naciones a nivel global. En Latinoamérica, el 80% de las organizaciones tiene dificultades para cubrir vacantes debido a la escasez de talento en ciberseguridad, lo cual afecta tanto al sector privado como al público (Fortinet et al., 2024). Por lo tanto, la capacitación integral de ingenieros de sistemas militares en el campo de la ciberdefensa representa un bien público estratégico.

La vulnerabilidad de las instituciones se evidencia en el crecimiento exponencial de ciberataques en Colombia desde la perspectiva local. Los intentos aumentaron de 1.362 millones

a 36.000 millones entre 2021 y 2024, lo que representa un reto para la seguridad nacional que va más allá de lo meramente técnico. Esta circunstancia justifica la importancia de desarrollar programas de estudio militar enfocados en promover habilidades humanas en resiliencia digital, operaciones híbridas, criptografía y Ciberinteligencia.

Tabla 2

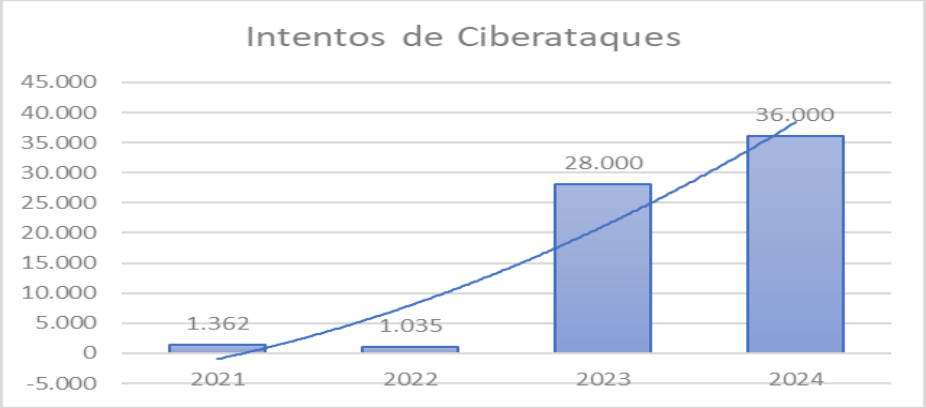
Indicadores de Seguridad de la Información y Ciberseguridad

Año	Ataques Cibernéticos (Millones)	Presupuesto Invertido a SI y CS
2021	1.362	341 Millones
2022	1.035	425 Millones
2023	28.000	440 Millones
2024	36.000	510 Millones

Nota. Inversiones realizadas por los bancos y efectividad de las estrategias puestas en marcha para fortalecer la seguridad digital. Adaptada de *"Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CS)"* [Texto] (Colombia, S. F. 2024), https://www.superfinanciera.gov.co/publicaciones/10113397/informes-y-cifrasinformesindicadores-de-seguridad-de-la-informacion-y-ciberseguridadindicadores-de-seguridad-de-la-informacion-y-ciberseguridad-10113397/

Figura 2

Evolución de Ciberataques.



Nota. Crecimiento de los ciberataques entre 2021 al 2024, evidenciando una alta vulnerabilidad institucional y un desafío para la seguridad nacional. Adaptada de *"Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CS)"* [Imagen] (Colombia, S. F. 2024), https://www.superfinanciera.gov.co/publicaciones/10113397/informes-y-cifrasinformesindicadores-de-seguridad-de-la-informacion-y-ciberseguridadindicadores-de-seguridad-de-la-informacion-y-ciberseguridad-10113397/

En resumen, este trabajo monográfico es de vital importancia, ya que logra analizar un vacío importante entre la ciberdefensa y la doctrina militar, proponiendo soluciones educativas. La perspectiva holística facilitará que el Ejército Nacional incremente su potencial institucional y contribuya a la creación de un modelo doctrinal apropiado para lo digital, asegurando así la protección de la soberanía y la seguridad del país, también ayuda a salvar a la sociedad civil de los riesgos emergentes que surgen con el uso del ciberespacio como escenario de confrontación.

En consecuencia, la razón de ser de esta investigación radica en la urgente necesidad de adaptar y actualizar la doctrina militar a las amenazas y dinámicas específicas del entorno cibernético, garantizando así una respuesta soberana, coordinada y eficaz frente a los nuevos tipos de conflictos que caracterizan al siglo XXI.

Objetivos

Objetivo General

Realizar una revisión sistemática de la literatura sobre guerra cibernética en currículos y bases doctrinales, para formular una propuesta curricular que fundamente la inclusión de la asignatura de guerra cibernética en la doctrina militar colombiana.

Objetivos Específicos

Identificar la consecuencia de la guerra cibernética en la doctrina militar de Colombia y cómo se refleja en el desarrollo de tácticas defensivas innovadoras y contextos operativos contemporáneos.

Establecer las nociones doctrinales, pedagógicas y tecnológicas que respalden la inclusión de la guerra cibernética como materia en el entrenamiento militar, de acuerdo con las políticas educativas y de defensa nacional.

Clasificar y sistematizar las fuentes doctrinales, académicas y científicas pertinentes para establecer un marco de referencia que apoye la propuesta curricular en el ámbito de ciberdefensa.

Estructuración del Trabajo de Investigación

Definición del Problema

Adaptarse a las nuevas circunstancias estratégicas que surgen del ciberespacio y del entorno digital como nuevo campo de confrontación es el reto actual al que se enfrenta la doctrina militar colombiana. Las amenazas cibernéticas han evolucionado de ser eventos aislados a formar parte esencial de los conflictos contemporáneos, impactando la infraestructura crítica, la soberanía nacional y la estabilidad institucional del Estado. Sin embargo, las Fuerzas Militares de Colombia no han integrado del todo el tema de guerra cibernética a su doctrina, ni como un eje educativo ni como una asignatura estructurada en sus planos curriculares, a pesar de los avances normativos y tecnológicos en el campo de la ciberseguridad y la ciberdefensa (Realpe Díaz, 2019; Rivera Alturo, L. M., & Hernández García, S. A., 2023).

La ausencia de esta formación curricular produce vacíos en la preparación del personal militar, que, a pesar de que desarrolla habilidades operativas y tácticas, aún no posee una capacitación integral que incorpora los principios técnicos, doctrinales y éticos necesarios para encarar las amenazas digitales. Por fin, existe una discrepancia entre la realidad estratégica del ciberespacio y las prácticas doctrinales clásicas de enseñanza, que aún se concentran en los dominios marítimos, aéreos y terrestres (Peña Suárez, 2023).

Además, gracias a los avances de la tecnología y las políticas mundiales en materia de defensa, el ciberespacio se ha convertido en un lugar fundamental para las acciones militares. Esto requiere la formación de habilidades humanas centradas en prevenir, responder y recuperarse frente a los ciberataques (Gamboa, J. A., 2023). Por otra parte, la educación militar tiene que satisfacer el deber institucional de fortalecer la soberanía digital y la cultura de

ciberseguridad en el país, así como también la de proteger los sistemas informáticos como requerimiento operativo.

Conforme a la revisión sistemática generada al documento de (Barrero, J. C., 2025) - Política de Educación para la Fuerza Pública 2021-2026, es esencial promover la inclusión de capacidades doctrinales y tecnológicas militares en los planes educativos, con el propósito de que la educación militar esté en sintonía con los desafíos contemporáneos en términos de defensa. Sin embargo, en la práctica persisten limitaciones pedagógicas y metodológicas para abordar la guerra cibernética como un fenómeno de múltiples dimensiones que combina conocimientos técnicos con inteligencia estratégica y principios institucionales en el contexto academico. Por lo tanto, es necesario analizar los principios doctrinales, tecnológicos y pedagógicos que respalden la incorporación de la guerra cibernética como asignatura en los programas de capacitación y actualización para las Fuerzas Militares. El objetivo es reforzar la capacitación integral de los mandos ante las nuevas amenazas del siglo XXI.

Descripción del Problema

Contexto y Relevancia

El ciberespacio se ha establecido hoy en día como un escenario clave de confrontación, lo que cambia radicalmente la naturaleza de los conflictos modernos. Las operaciones han dejado de circunscribirse a los dominios aéreo, marítimo o físico y ahora abarcan el ámbito digital, donde se llevan a cabo acciones de desinformación, espionaje, ataques dirigidos contra infraestructuras críticas y sabotaje (Valeriano, B., & Maness, R., 2015). El nuevo escenario ha originado lo que se conoce como guerra cibernética, un fenómeno de múltiples dimensiones que requiere de doctrinas adaptables, instituciones con capacidades sólidas y personal altamente

calificado, capaz de prever y contrarrestar las amenazas emergentes (Mozo Rivera, O., & Ardila Contreras, J. V., 2022).

Las potencias militares más importantes del mundo han integrado la ciberdefensa como un elemento fundamental de sus planos de seguridad nacional, al darse cuenta de la naturaleza asimétrica y disruptiva de las confrontaciones digitales (Arquilla, J., & Ronfeldt, D., 2007). No obstante, en el contexto de América Latina todavía hay importantes rezagos, tanto en la creación de marcos doctrinales integrales como en la capacitación del talento humano especializado en defensa digital (Antonio, J. M, 2021). Este panorama demuestra con urgencia la necesidad de robustecer las capacidades doctrinales e institucionales para afrontar los peligros que surgen en el ciberespacio.

De acuerdo a (Centro de Doctrina del Ejército, 2020) la Doctrina Damasco en Colombia es un intento de modernizar la estructura, los procedimientos y las operaciones del Ejército Nacional, al considerar formalmente al ciberespacio como un nuevo ámbito de confrontación estratégica. No obstante, aún persisten limitaciones doctrinales y restricciones en la conexión entre las políticas de defensa, la doctrina institucional y los programas de formación para ingenieros de sistemas militares. Estos últimos tienen un papel fundamental en la protección de los activos digitales del Estado. Según (Realpe Diaz, M. E., & Cano Martínez, J. J., 2020), esta falta de coordinación conlleva una reducción en la habilidad para prever, contrarrestar y responder eficazmente a los ciberataques que ponen en riesgo la seguridad nacional y la estabilidad institucional.

Causas del Problema

Las causas interconectadas han sido identificadas como las raíces estructurales de la complejidad. En primer lugar, se observa la ausencia de una doctrina militar que esté totalmente adaptada al ciberespacio y que contenga principios, protocolos y tácticas específicas para orientar la acción militar en este campo. En segundo lugar, han surgido profesionales con un elevado nivel técnico, pero con una preparación doctrinal, estratégica y ética insuficiente, debido a la débil articulación entre los programas de formación militar y las necesidades doctrinales actuales.

De igual manera, la ausencia de sistematización de las obras doctrinales y científicas más recientes dificulta la creación de un marco normativo actualizado que guíe la transformación del Ejército Nacional en términos doctrinales y educativos frente a las amenazas digitales (Page et al., 2021). En última instancia, la insuficiencia de personal con alta especialización en ciberdefensa militar disminuye la efectividad y sostenibilidad de las unidades cibernéticas establecidas en el país, lo que limita la capacidad operativa ante incidentes complejos (Organización de los Estados Americanos O.E.A, 2016).

Consecuencias

Estos déficits generan efectos en diferentes niveles. La ausencia de normas actualizadas para la defensa en el ciberespacio, desde una perspectiva doctrinal, provoca que las respuestas a las amenazas digitales sean fragmentadas, reactivas y aisladas. La formación de los ingenieros de sistemas militares no abarca habilidades completas en ética profesional, derecho internacional vigente, inteligencia digital y ciberseguridad; estos son elementos fundamentales para encarar los

desafíos de la guerra cibernética (Foro Económico Mundial, 2024). En el ámbito estratégico, la ausencia de habilidades firmes debilita la defensa del país frente a ciberataques complejos, lo que repercute en operaciones militares, infraestructura crítica y la confianza institucional (Rid, T., 2011). Por último, en el ámbito político-social, la fragilidad del ciberespacio pone en peligro la soberanía estatal y expone a los ciudadanos a peligros que provienen de la desconfianza pública y de la interrupción de servicios fundamentales (Foro Económico Mundial, 2024).

Importancia del Estudio

Resulta fundamental, en este contexto, llevar a cabo una revisión sistemática de la bibliografía correspondiente al periodo 2020-2025, empleando el método PRISMA 2020. Esto facilitará el análisis de las contribuciones doctrinales y teóricas más nuevas acerca de cómo la guerra cibernética afecta la doctrina militar en Colombia. Esta investigación tiene como finalidad detectar vacíos, tendencias y sugerencias relevantes para modernizar la doctrina y robustecer el currículo de los programas destinados a formar ingenieros de sistemas de las Fuerzas Militares.

Las conclusiones de este estudio ayudarán a formular estrategias que incorporan los elementos técnicos, doctrinales, éticos y legales, los cuales son fundamentales para abordar los retos del entorno digital. Además, los resultados podrán ser utilizados para desarrollar políticas públicas y directrices institucionales que mejoren la coordinación entre las estrategias nacionales de ciberseguridad y los planos educativos en el ámbito de defensa. Así, se fomentará el desarrollo del cuerpo doctrinal que esté en línea con las necesidades actuales de defensa nacional, asegurando una respuesta táctica, ética y efectiva ante los peligros de la guerra cibernética.

Formulación del Problema

¿De qué manera la inclusión de la guerra cibernética en la doctrina militar colombiana puede contribuir al fortalecimiento de las competencias estratégicas, tecnológicas y éticas del personal militar y cuáles son los fundamentos pedagógicos y doctrinales que sustentan su inclusión como asignatura en la actualización doctrinal?

Marco Referencial

Antecedentes

En años recientes, la literatura científica de Colombia ha comenzado a abordar con mayor profundidad el fenómeno de la guerra cibernética y su impacto en las doctrinas militares, reconociendo que el ciberespacio se está transformando progresivamente en un nuevo campo de confrontación estratégica. (Suarez, J. S., 2023) es uno de los que más ha aportado a este asunto. En su artículo "Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital", lleva a cabo un detallado análisis de documentos que muestran las falencias institucionales en términos de infraestructura, capacidad técnica y actualización doctrinal, lo que pone de manifiesto la necesidad de actualizar los sistemas de defensa militar frente a nuevas amenazas digitales (Suarez, J. S., 2023). Además, (Pacheco, J. A., 2022) destaca la importancia de establecer un marco legal sólido que apoye las medidas de ciberdefensa y ciberseguridad en Colombia. El escritor de su investigación “La importancia de una Ley de ciberseguridad y ciberdefensa para Colombia” argumenta que la falta de leyes concretas restringe la habilidad del Estado para reaccionar y crear vacíos en la coordinación entre doctrina militar, política pública y acciones de ciberdefensa. Autores como (Ringas, E. E., Kerttunen, M., & Spirito, C., 2014) destacan que la ciberseguridad debe integrarse como un campo formal de estudio en la educación militar. Este estudio, a pesar de estar enfocado en un contexto internacional, brinda enseñanzas estratégicas que pueden ser implementadas en Colombia, particularmente en lo que respecta a la planificación, coordinación y realización de acciones ofensivas y defensivas en el ciberespacio (Mozo Rivera, O., & Ardila Contreras, J. V., 2022).

Igualmente, (Arciniegas Londoño, L., & Arcila Martínez, L. Y., 2023) tratan el papel del Ejército de Liberación Nacional (ELN) en los ámbitos cognitivo, terrestre y cibernético,

mostrando la manera en que actores no estatales utilizan estrategias híbridas que integran acciones digitales y físicas. Este análisis subraya la necesidad de que la doctrina militar colombiana contemple puntos de vista multidominio y el desarrollo de capacidades adaptativas frente a amenazas no tradicionales.

Desde hace una década se ha generado un incremento continuo en la investigación acerca de la guerra cibernética y su impacto en las doctrinas militares. Según estudios globales, como los realizados por (Fortinet et al., 2024) y el Foro Económico Mundial (2024), las amenazas en el ciberespacio han sido clasificadas como el mayor peligro para la estabilidad de las instituciones. Estos estudios muestran datos y tendencias que confirman el incremento acelerado de las brechas en materia de seguridad e intentos de intrusión. La (Organización de los Estados Americanos O.E.A, 2016) constató un aumento notable de la actividad ofensiva digital en América Latina, lo que ha fomentado agendas tanto públicas como privadas orientadas a fortalecer el equipo laboral dedicado a la ciberseguridad.

En el contexto nacional, estudios académicos y técnicos (Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiro, J. A., 2020); (Realpe Diaz, M. E., & Cano Martínez, J. J., 2020) han analizado la manera en que las Fuerzas Militares de Colombia se han ajustado ante amenazas no convencionales. Algunos de los hallazgos más relevantes son el establecimiento de unidades especializadas y la primera aproximación normativa a través de instrumentos como la Doctrina Damasco (Centro de Doctrina del Ejército, 2020). Sin embargo, estos estudios están de acuerdo en que hay vacíos en la articulación entre doctrina, capacitación y tecnología: generalmente, la integración de habilidades cibernéticas es fragmentada, reactiva y con limitaciones en términos de interoperabilidad y recursos humanos especializados.

Los reportes (Fortinet et al., 2024) ofrecen cifras sobre el aumento de los intentos de ataque, en Colombia, se registraron 12.000 millones durante 2023 y 36.000 millones en 2024, lo que refleja una tendencia que necesita respuestas doctrinales y educativas más veloces. Simultáneamente, las comparaciones con estándares internacionales (como el Manual de Tallin y los procedimientos de EE. UU.) permiten identificar prácticas adecuadas para incorporar la ciberdefensa como un ámbito operativo y formativo. Los estudios relacionados con la educación y capacitación en ciberseguridad alertan acerca de la disparidad entre lo que se demanda en términos de perfiles especializados y lo que el sector público ofrece a un nivel curricular. Un descubrimiento que destaca la importancia de dirigir los programas de formación desde las academias militares es el hecho de que el 80% de las organizaciones en Latinoamérica informó problemas para llenar puestos vacantes en ciberseguridad (Fortinet et al., 2024). En resumen, las investigaciones realizadas señalan tres patrones que se repiten: la incorporación gradual, aunque irregular, de habilidades cibernéticas en entidades militares; el crecimiento exponencial de las amenazas entre 2020 y 2025; y la falta de formación que impacte en la sostenibilidad operativa de estas capacidades. Su contribución consiste en mostrar ejemplos a nivel regional (Colombia/Latinoamérica) y resaltar los desafíos doctrinales y tecnológicos para la incorporación de IA en las operaciones defensivas.

En su artículo titulado "Ejes temáticos estratégicos en seguridad y defensa en Colombia", (Acevedo Navas, C., & Fernández Osorio, A. E, 2023) determinan que la ciberdefensa y la ciberseguridad son elementos esenciales de la agenda nacional de seguridad. Esta identificación confirma la pertinencia de analizar el impacto que han tenido estos cambios en la doctrina militar desde 2020 hasta 2025, en el contexto de los desafíos emergentes en el ámbito digital y las políticas del Estado.

En general, estos antecedentes muestran una tendencia en aumento hacia la inclusión del ciberespacio en la planificación y aplicación de la defensa nacional. Asimismo, enfatizan la importancia de llevar a cabo una revisión sistemática, como se plantea en esta investigación, que contempla los descubrimientos más recientes y posibilita medir el nivel de adecuación doctrinal de las Fuerzas Militares colombianas ante los retos que impone la guerra cibernética moderna.

Marco Teórico

Una profunda transformación en las doctrinas que orientan la planificación estratégica de los Estados y en las formas de confrontación ha caracterizado el desarrollo de los conflictos armados actuales. La aparición del ciberespacio como un nuevo campo de batalla, así como la inclusión de tecnologías emergentes, entre ellas la inteligencia artificial (IA), la automatización de sistemas y la Ciberinteligencia, han dado lugar a una atmósfera bélica más compleja, difusa y multidimensional. En este escenario, la guerra cibernética se presenta como un suceso disruptivo que desafía los principios tradicionales de la doctrina militar y obliga a replantear los conceptos de soberanía, amenaza y uso legítimo de la fuerza.

Este panorama requiere una reflexión profunda sobre la naturaleza del conflicto, los deberes éticos en las operaciones digitales, la capacitación de los miembros militares y el nivel de soberanía nacional en situaciones interconectadas a nivel mundial. También es necesario revisar los principios tradicionales que rigen el uso de la fuerza.

Este estudio, para analizar esta transformación doctrinal, se fundamenta en tres ejes teóricos que describen el impacto de la guerra cibernética en las doctrinas militares contemporáneas. Estos son los tres enfoques:

El enfoque de dominios múltiples.

La visión del ciberpoder.

La teoría de la guerra híbrida.

Cada uno de estos marcos teóricos brinda una perspectiva adicional sobre cómo las operaciones en el ciberespacio están transformando la estrategia y el pensamiento militar del siglo XXI.

Teorías de la Educación y Diseño Curricular para la Defensa

El cuarto eje teórico está basado en las teorías actuales acerca de la educación militar y el diseño curricular, que subrayan la importancia de ajustar los procesos educativos a los nuevos contextos de seguridad. Según (Ringas, E. E., Kerttunen, M., & Spirito, C., 2014), la ciberseguridad tiene que ser un área de estudio formal en la educación militar. Para ello, es necesario tener planos de estudio que se enfoquen en el desarrollo de habilidades técnicas, estratégicas y éticas para operar en el ciberespacio. Este punto de vista se basa en el principio de que la eficacia de una doctrina militar moderna depende, en gran medida, de su implementación eficaz en programas de capacitación.

En el caso de Colombia, es imprescindible una reestructuración curricular para incluir la asignatura de guerra cibernética en la doctrina Damasco. Según esta perspectiva, la educación militar debe avanzar de paradigmas tradicionales que se fundamentan en la repetición de tácticas convencionales a métodos basados en competencias, las cuales fomentan habilidades para el pensamiento crítico, la adaptabilidad y la solución de problemas en contextos digitales

cambiantes. Dentro de este contexto, la asignatura de guerra cibernética no es simplemente técnica; además, necesita una comprensión minuciosa de los componentes estratégicos, éticos y geopolíticos que la transforman en un nuevo tipo de conflicto asimétrico (Realpe Díaz, 2019). Esta aproximación haría posible delinear competencias específicas en ciberdefensa, operaciones en el ciberespacio y ciberinteligencia, que estarían alineadas con los principios doctrinales Damasco y cumplirían con las necesidades operativas del Ejército Nacional.

De igual manera, (Gamboa, J. A., 2023) enfatiza que, para este nuevo prototipo de defensa digital, resulta necesario desarrollar una doctrina cibernética propia que esté fundamentada en la soberanía tecnológica, la seguridad de la información y la capacidad de adaptación.

Guerra Híbrida y Conflicto Asimétrico

Para entender la complejidad de los conflictos actuales, uno de los conceptos más importantes es el de guerra híbrida. Según Hoffman (2009), se define como la convergencia de medios no convencionales y convencionales, que incluyen el ciberespacio, las operaciones informacionales, la guerra psicológica y las acciones irregulares. Todo esto conduce a situaciones de conflicto que son asimétricas y multidimensionales. Esto posibilita entender que las amenazas digitales no operan de forma independiente, sino que se integran en estrategias globales que combinan ataques a infraestructuras esenciales, manipulación informativa y coacción política.

Siguiendo la revisión sistemática, Clarke y Knake (2010) sostienen que la guerra cibernética no es una categoría independiente; por el contrario, es una forma híbrida que

combina operaciones de espionaje, sabotaje, alteraciones de datos e incursiones a sistemas informáticos con fines estratégicos. Estos tienen el potencial de poner en peligro la soberanía del Estado, socavar la confianza en las instituciones y hacer que las fuerzas armadas sean menos capaces de responder a amenazas difusas. Asimismo, su naturaleza anónima y la dificultad de atribuirlas las convierten en herramientas valiosas para actores estatales y no estatales, que tienen la capacidad de alterar el equilibrio del poder sin necesidad de entrar en un conflicto directo.

En este contexto, la guerra híbrida demuestra que las maneras de conflicto del siglo XXI superan las fronteras entre la guerra y la paz, lo civil y lo militar, así como lo digital y lo físico. Esto requiere doctrinas adaptativas y flexibles que incorporen elementos informáticos, psicológicos y tecnológicos.

Dominios Múltiples y Operaciones Conjuntas

La perspectiva de dominios múltiples, el segundo eje teórico, sugiere una interpretación unificada del conflicto moderno, en la que el éxito operacional está condicionado por la coordinación simultánea de acciones en diversos ámbitos: mar, aire, tierra, espacio y ciberespacio. Según Mahnken (2011), el dominio cibernético debe ser visto como un elemento operativo fundamental, no meramente como una asistencia técnica, pues su control tiene la capacidad de determinar cómo se llevan a cabo las operaciones militares en la actualidad.

La literatura muestra una controversia conceptual sobre la condición del ciberespacio. Hay autores que lo ven como una expansión de los territorios tradicionales, mientras que otros lo perciben como un nuevo campo de batalla con sus propias normas. Healey (2024) propone un marco categórico con el objetivo de diferenciar las operaciones cibernéticas según su propósito

(por qué), localización (dónde) y tiempo (cuándo). Esto permite reconocer sus efectos doctrinales y su relevancia en términos estratégicos.

Ciberpoder y Dinámica Estatal

El tercer eje teórico se basa en la idea de ciberpoder, que fue formulada por (Libicki, M. C., 2009) y (Nye, J. S., 2010). Estos autores describen el ciberpoder como la habilidad de un Estado para extender su influencia y poder a través del ciberespacio, con el propósito de persuadir, coaccionar o negar capacidades. El ciberpoder cambia las relaciones internacionales y redefine los instrumentos de política exterior, ya que posibilita la implementación de medidas estratégicas sin necesidad de emplear la fuerza física.

El tercer eje teórico se basa en la idea de ciberpoder, que fue formulada por (Libicki, M. C., 2009) y (Nye, J. S., 2010). Estos autores describen el ciberpoder como la habilidad de un Estado para extender su influencia y poder a través del ciberespacio, con el propósito de persuadir, coaccionar o negar capacidades. El ciberpoder cambia las relaciones internacionales y redefine los instrumentos de política exterior, ya que posibilita la implementación de medidas estratégicas sin necesidad de emplear la fuerza física.

El desarrollo de habilidades ofensivas y defensivas en el ciberespacio influye directamente en la elaboración doctrinal, a la vez que plantea nuevos desafíos jurídicos. Este conflicto, entre la necesidad de una reacción rápida y flexible frente a riesgos invisibles y la demanda de seguridad jurídica, pone de manifiesto la relevancia de crear doctrinas éticas y versátiles que integren el Derecho Internacional Humanitario con la eficacia operacional en el terreno digital.

Recapitulación Doctrinal

La intersección de la guerra híbrida, el ciberpoder y las operaciones multidominio hace posible entender que la doctrina militar actual debe verse como un sistema en movimiento y capaz de adaptarse, donde se entrelazan la normativa, la estrategia y la tecnología. En el marco de Colombia, esta síntesis supone un cambio de la doctrina que se enfoca en los dominios físicos tradicionales a una perspectiva integral y multidominio, con el objetivo de extender la gobernanza del ciberespacio y la interoperabilidad internacional, así como de reforzar las competencias éticas y técnicas en los integrantes de las fuerzas militares. Desarrollo de habilidades técnicas y éticas en el personal militar. Únicamente a través de esta perspectiva será factible establecer una defensa nacional sólida y resiliente, que tenga la capacidad de reaccionar eficazmente ante los retos asimétricos del siglo XXI.

Educación Militar y Formación en Ciberdefensa: Una Perspectiva Pedagógica

La educación militar está atravesando una profunda transformación que tiene como objetivo incorporar la tecnología, la innovación y la investigación como fundamentos en la formación del nuevo profesional de las Fuerzas Militares (Peña Suárez, 2023). En esta dirección, el hecho de incluir la asignatura de guerra cibernética como materia no solo responde a una necesidad técnica, sino también pedagógica, porque fomenta un aprendizaje que se basa en solucionar problemas, simular y tomar decisiones en contextos virtuales.

Según (Gamboa, J. A., 2023), la capacitación en habilidades cibernéticas y digitales refuerza el liderazgo militar, ya que posibilita que los oficiales del mañana entiendan las repercusiones doctrinales, operativas y morales de la utilización de tecnologías informáticas en la

defensa nacional. De acuerdo con esto, la Política de Educación para la Fuerza Pública 2021–2026 determina que los programas educativos deben incluir el empleo de simuladores, aprendizaje en equipo y métodos activos para fomentar las capacidades en ciberdefensa y seguridad digital.

Desde el punto de vista pedagógico, esta integración curricular debe fundamentarse en las bases del aprendizaje significativo y del constructivismo, para que el saber se utilice en contextos reales y simulados de defensa (Ausubel, D., 1983), en vez de ser memorizado. En consecuencia, la educación militar debe trascender la enseñanza técnica y convertirse en un proceso que sea tanto práctico como reflexivo, con el fin de formar líderes que puedan manejar el ciberespacio.

Fundamentos Para la Inclusión Curricular de la Asignatura de Guerra Cibernética

La actualización curricular de las Fuerzas Militares debe responder a los retos emergentes de la defensa nacional y las dinámicas globales del conflicto. Según (Barrero, J. C., 2025) que referencia la Política de Educación para la Fuerza Pública 2021-2026, la incorporación de nuevos contenidos en el currículo debe basarse en el desarrollo de competencias, el impulso de la investigación aplicada y la relevancia social.

Hay tres factores esenciales que respaldan la idea de que la asignatura de guerra cibernética sea una disciplina:

Doctrinal, al consolidar el ciberespacio como dominio operativo reconocido dentro de la defensa nacional.

Tecnológica, al fortalecer las capacidades de ciberseguridad y Ciberinteligencia.

Pedagógica, porque fomenta un aprendizaje que es activo y crítico, fundamentado en la simulación, el trabajo colaborativo y la ética de la institución.

(Realpe Díaz, 2019) propone que la formación en ciberdefensa debe integrarse desde los niveles más básicos hasta los de mayor rango de la carrera militar, conectando lo teórico con lo práctico y con el análisis aplicado. De igual manera, la Escuela Superior de Guerra propone que la doctrina militar tiene que renovarse de acuerdo con los nuevos contextos estratégicos y tecnológicos, poniendo en primer lugar a la educación como herramienta para transformar las instituciones.

Marco Conceptual

Debido a los avances tecnológicos, la naturaleza de los conflictos actuales en términos de seguridad y defensa se ha transformado radicalmente, creando nuevas condiciones estratégicas que van más allá de las áreas convencionales: mar, aire, tierra y espacio. El panorama actual, caracterizado por la interconexión mundial y la dependencia de sistemas digitales, ha generado el nacimiento de nuevas amenazas que desafían las doctrinas militares ya establecidas y obligan a los países a meditar sus estrategias en cuanto a seguridad nacional y defensa.

Por ende, el marco conceptual actual tiene como objetivo establecer definiciones operativas que sustenten los objetivos o ejes analíticos de la investigación, incorporando los conceptos de guerra cibernética, ciberdefensa, doctrina militar, educación militar, seguridad y defensa nacional, ciberespacio, dominio cibernético, resiliencia digital, Ciberinteligencia, operaciones híbridas y contexto colombiano. Estos términos sirven como fundamento teórico y

metodológico para comprender la necesidad de incluir la asignatura de guerra cibernética dentro del sistema educativo militar de Colombia.

Guerra Cibernética

(Rodríguez, P. A., 2025) describe la guerra cibernética como el uso deliberado de acciones ofensivas y defensivas en el ciberespacio, ya sea por parte de actores estatales o no estatales, con el objetivo de perjudicar, modificar funciones estratégicas o ejercer influencia sobre las decisiones del enemigo. Este tipo de guerra, a diferencia de los conflictos convencionales, se distingue por su invisibilidad, rapidez, anonimato y dificultad para atribuirlo a una parte específica, lo cual supone nuevos retos en cuanto a ética, estrategia y ley. Las operaciones cibernéticas pueden abarcar la manipulación de información, el espionaje digital, los ataques a infraestructuras fundamentales o la interferencia en comunicaciones militares. En el contexto Colombiano, el (Departamento Nacional de Planeación, 2016) - CONPES 3854 considera en el marco colombiano la guerra cibernética como uno de los elementos esenciales de las operaciones de información, que incluyen habilidades de Ciberinteligencia, ciberdefensa y reacción frente a incidentes y que son un componente fundamental de la estrategia para la seguridad nacional.

Ciberdefensa y Ciberseguridad

Según (Suarez, J. S., 2023), la ciberseguridad o ciberdefensa comprende las acciones, tecnologías y políticas que buscan resguardar los sistemas digitales, la información y las infraestructuras esenciales de ataques, sabotajes y accesos no permitidos. Su propósito es

garantizar la confidencialidad, la integridad y el acceso a los recursos digitales, según el CONPES 3701 quien especifica los lineamientos de política para ciberseguridad y Ciberdefensa, (Departamento Nacional de Planeación, 2011)

El aspecto militar de la ciberseguridad es la ciberdefensa. De acuerdo con (Pacheco, J. A., 2022), esto supone el fortalecimiento de habilidades ofensivas y defensivas en el ciberespacio para proteger los intereses estratégicos del Estado y garantizar la operación continua de las fuerzas armadas. Esta disciplina abarca la planificación de operaciones en el ámbito virtual, así como la inteligencia digital y la capacidad de respuesta ante ataques cibernéticos, además de proteger las infraestructuras militares críticas.

Doctrina Militar

La doctrina militar puede ser caracterizada como un conjunto sistemático de principios, reglas, procedimientos y valores que orientan la preparación, el empleo y el mantenimiento de las Fuerzas Armadas durante el cumplimiento de su misión institucional (Ejército nacional de Colombia, 2017). De igual manera, (Acevedo Navas, C., & Fernández Osorio, A. E, 2023) manifiestan que la doctrina militar es un término que se refiere a los principios, conceptos, procesos y regulaciones que guían la creación, organización y aplicación de las Fuerzas Armadas. Su función es ofrecer un marco conceptual que orienta la toma de decisiones estratégicas y operativas. La aparición del ciberespacio como un nuevo escenario de enfrentamiento hace necesario actualizar y reevaluar la doctrina actual, incorporando puntos de vista de diferentes disciplinas que engloban la inteligencia digital, la ciberdefensa y las capacidades tecnológicas en el planeamiento militar.

Una doctrina militar moderna no puede limitarse a ser un documento teórico; debe reflejarse concretamente en los planes de estudio de las Fuerzas Armadas. De acuerdo con la revisión sistemática de la literatura, (Peña Suárez, 2023) señala que para reformar la doctrina no basta con incorporar tecnologías novedosas, sino que también se requiere reestructurar los procedimientos de enseñanza, las estructuras organizacionales y las nociones estratégicas. Así, la doctrina militar de Colombia necesita una adaptación para afrontar un escenario de seguridad con amenazas invisibles, asimétricas y transnacionales. Esto exige, de manera obligatoria, una reestructuración de sus programas de formación para que la asignatura de guerra cibernética se integre como un componente esencial del conocimiento militar contemporáneo.

Educación Militar

La educación militar tiene como objetivo la formación integral de los miembros de las Fuerzas Armadas, fundamentada en los principios del liderazgo, la ética, la disciplina y la profesionalización, con el propósito de asegurar que se lleven a cabo las misiones constitucionales. La doctrina militar no se encuentra aislada; por el contrario, se concreta y se reproduce a través de procesos educativos organizados dentro de las Fuerzas Armadas. La educación militar, de acuerdo con (Acevedo Navas, C., & Fernández Osorio, A. E, 2023), es el medio esencial a través del cual se comunican los principios doctrinales a las nuevas generaciones de oficiales y suboficiales, asegurando así la consistencia en las operaciones y la unidad de criterio en las acciones militares.

Ejemplos de programas educativos que actúan como medios para la socialización de doctrinas son la Escuela Superior de Guerra, las escuelas de armas y los centros educativos

militares. En ellos, los líderes militares en formación incorporan los principios, procesos y valores que guían la acción militar. En gran medida, se evalúa la efectividad de una doctrina según su inclusión apropiada en los planos de formación, donde se expresa mediante simulaciones operativas, habilidades específicas y prácticas tácticas.

Finalmente, la actualización de los contenidos del currículo es una herramienta esencial para el avance doctrinal. El sistema educativo militar necesita modernizar su contenido para preparar a sus integrantes ante los nuevos retos, como las amenazas híbridas y asimétricas o el ciberespacio. La incorporación de materias especializadas, como la guerra cibernética, no es solo una adición a nivel temático; también implica una reconfiguración doctrinal que tiene en cuenta el cambio en la naturaleza de los conflictos actuales. Esta sinergia entre educación y doctrina asegura que las Fuerzas Militares mantengan su relevancia operativa y capacidad de respuesta ante un entorno de seguridad en constante cambio.

Seguridad y Defensa Nacional

Como sostiene (Acevedo Navas, C., & Fernández Osorio, A. E, 2023), la seguridad nacional comprende todas las políticas, acciones y capacidades que garantizan la defensa de los intereses estratégicos de un país frente a amenazas externas e internas, así como su soberanía y la integridad territorial. En este contexto, la defensa nacional es el componente militar de esa seguridad y su propósito es evitar y hacer frente a los ataques mediante la organización, el equipamiento y el uso de las fuerzas armadas. Históricamente, estas iniciativas se enfocaban en amenazas convencionales; sin embargo, la digitalización a nivel mundial ha traído riesgos asimétricos que no necesitan una presencia física para causar daños estratégicos.

Ciberespacio

(Rodríguez, A. G., 2015) sostiene que el ciberespacio es un espacio global constituido por sistemas informáticos, redes interconectadas, infraestructuras digitales y dispositivos tecnológicos que hacen posible la divulgación de información. Aunque este campo es inmaterial, influye de manera directa en las áreas política, económica, militar y social de las naciones. El carácter abierto, variable y de control difícil ha posibilitado que los actores del Estado y no estatales desarrollen capacidades de defensa y ofensiva, generando así un nuevo ámbito para la competencia estratégica.

Ciberespacio y Dominio Cibernético

El ciberespacio es el ambiente global interconectado conformado por redes digitales, sistemas de información y tecnologías que posibilitan la generación, intercambio y almacenamiento de datos (Rodríguez, A. G., 2015). En este entorno se encuentra el dominio cibernético, que es un espacio operativo e incluye infraestructuras críticas, redes y recursos informáticos relevantes para la seguridad nacional y la proyección del poder estatal. Su carácter estratégico lo convierte en una nueva área de maniobras militares equiparable a los dominios marítimo, terrestre, aéreo y espacial; esto implica contar con capacidades doctrinales y operativas específicas.

Resiliencia Digital

La resiliencia digital, que complementa este concepto, busca mantener la continuidad operativa y reducir los impactos críticos a través de la resistencia, la simulación y la recuperación

frente a eventos cibernéticos. En el campo militar, la resiliencia digital se refiere a la puesta en marcha de protocolos para la recuperación, sistemas de respuesta adaptables e infraestructuras redundantes con el propósito de garantizar que los servicios esenciales sigan funcionando a pesar de un ataque.

Ciberinteligencia

La Ciberinteligencia es un proceso tanto analítico como operativo que une la recolección, la elaboración, el análisis y la interpretación de datos digitales para predecir, identificar y reaccionar ante peligros en el ciberespacio. Según (Rodríguez, P. A., 2025), este elemento es esencial para tomar decisiones estratégicas, asignar ataques y planificar operaciones de ciberdefensa, ya que posibilita el reconocimiento de patrones de riesgo, actores hostiles y debilidades antes de que se concreten (López, A. F., & Velásquez, L., 2021).

Operaciones Híbridas

Las operaciones híbridas aparecen como una mezcla de tácticas irregulares, convencionales y cibernéticas que persiguen el objetivo de aprovechar las debilidades del oponente en varios dominios al mismo tiempo (Arciniegas Londoño, L., & Arcila Martínez, L. Y., 2023). Estas tácticas, empleadas por las Fuerzas Militares y grupos armados no estatales, tienen como objetivo provocar efectos desmedidos a través de la integración de operaciones digitales, informacionales, psicológicas y militares. El comportamiento del ELN y otros grupos insurgentes en el ciberespacio muestra que es necesario que la doctrina militar incorpore una

perspectiva multidominio que contemple tanto el componente cognitivo como el virtual (Arciniegas Londoño, L., & Arcila Martínez, L. Y., 2023).

Contexto Colombiano

La política nacional de seguridad digital según el (Ministerio de Defensa Nacional, 2020) en el CONPES 3995, sobre ciberdefensa y ciberseguridad, son ejemplos que muestran el avance en cuanto a ciberseguridad y ciberdefensa en Colombia (Departamento Nacional de Planeación, 2016). Sin embargo, diversos estudios han mostrado distinciones en la actualización de la doctrina, las competencias técnicas y el marco normativo. Este desfase pone de manifiesto que es necesario llevar a cabo un análisis sistemático para entender cómo la guerra cibernética ha influido en el desarrollo de la doctrina militar entre 2020 y 2025, así como qué modificaciones son requeridas para robustecer la defensa nacional ante amenazas digitales cada vez más complejas (Revista Científica General José María Córdova, 2020).

Para el Ejército nacional su curso de acción primordial, es tomar medidas tanto estratégicas, operativas y doctrinales para evitar vulnerabilidades en la institución debido al incremento de sostenido en la frecuencia y complejidad los ciberataques dirigidos contra las instituciones públicas y privadas de Colombia. (Díaz Acevedo, M., & Cremades Guisado, Á., 2024) resaltan que estos incidentes reflejan no solo la creciente dependencia de los servicios digitales, sino también a falta de madurez en los mecanismos de prevención, monitoreo y respuesta ante incidentes cibernéticos. La imagen que ilustra el artículo muestra un panorama del aumento de incidentes cibernéticos en el país, que durante 2022 afectaron a por lo menos 34 organizaciones con una variedad de ataques. Este aumento no solo indica una tendencia creciente

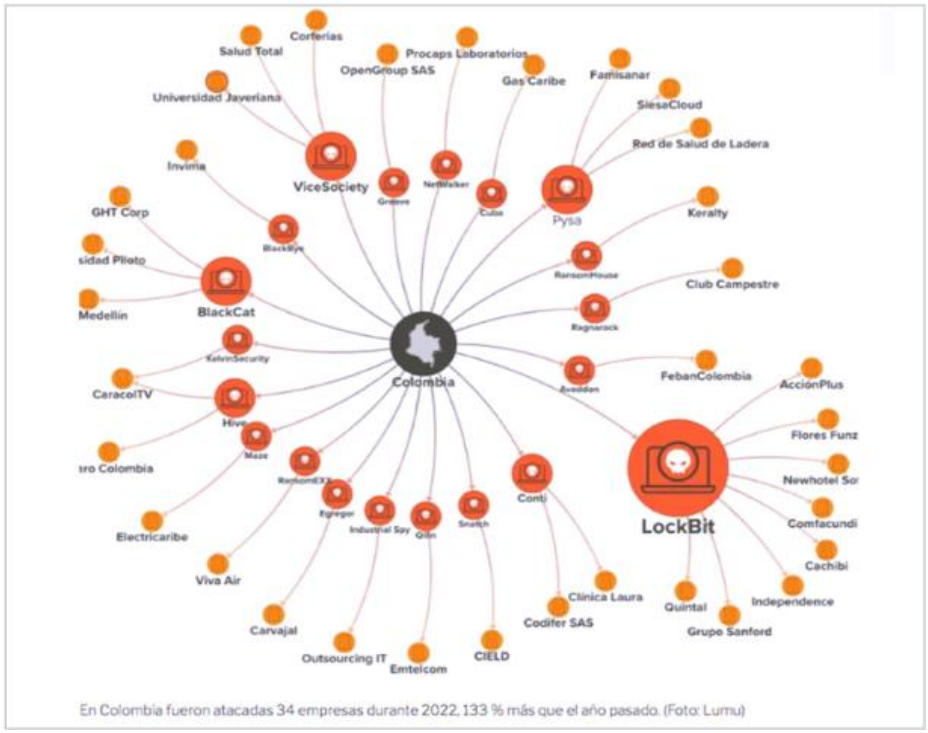
en la actividad maliciosa, sino que también evidencia la urgente necesidad de robustecer las habilidades nacionales para la defensa digital, tanto en términos técnicos como institucionales.

Para el Ejército nacional su curso de acción primordial, es tomar medidas tanto estratégicas, operativas y doctrinales para evitar vulnerabilidades en la institución debido al incremento de sostenido en la frecuencia y complejidad los ciberataques dirigidos contra las instituciones públicas y privadas de Colombia. (Díaz Acevedo, M., & Cremades Guisado, Á., 2024) resaltan que estos incidentes reflejan no solo la creciente dependencia de los servicios digitales, sino también a falta de madurez en los mecanismos de prevención, monitoreo y respuesta ante incidentes cibernéticos. La imagen que ilustra el artículo muestra un panorama del aumento de incidentes cibernéticos en el país, que durante 2022 afectaron a por lo menos 34 organizaciones con una variedad de ataques (Figura 3).

Este aumento no solo indica una tendencia creciente en la actividad maliciosa, sino que también evidencia la urgente necesidad de robustecer las habilidades nacionales para la defensa digital, tanto en términos técnicos como institucionales.

Figura 3

Ciberataque a Empresas Colombianas Año 2022



Nota. En Colombia fueron atacadas 34 empresas durante 2022, 133 % más que el año inmediatamente anterior. Tomada de *"Revisión del estado actual de la ciberseguridad en Colombia"* [Imagen] (Díaz Acevedo, M., & Cremades Guisado, Á., 2024), https://esdegrevistas.edu.co/index.php/resd/article/view/1999/5308

Estos antecedentes se constituyen como el fundamento para entender cómo ha evolucionado el ecosistema digital colombiano y la necesidad urgente de implementar estrategias integrales que aseguren la capacidad de adaptación cibernética del Estado.

Marco Legal

Para que la doctrina militar de Colombia se fortalezca en relación a una asignatura de guerra cibernética, es preciso contar con un sólido respaldo normativo que garantice su coherencia con los marcos legales vigentes. Este respaldo legislativo no solamente otorga legitimidad al procedimiento de reforma del currículo en las instituciones militares, sino que también establece los fundamentos para una educación integral, ética y acorde a las disposiciones nacionales en lo digital. El ciberespacio, un nuevo campo estratégico para las operaciones civiles y militares, representa uno de los desafíos más complejos del derecho actual. Dado que las tecnologías son transnacionales, evolucionan rápidamente y resulta difícil establecer responsabilidades, es esencial contar con un marco legal bien estructurado que incorpore instrumentos nacionales e internacionales con el fin de asegurar la soberanía de los estados, la protección digital y el respeto a los derechos esenciales.

Esto evidencia que existen fundamentos en el marco legal internacional para establecer principios comunes sobre el uso responsable del ciberespacio. Mientras que el marco jurídico de Colombia implementa estos principios mediante políticas, leyes y estrategias de defensa y seguridad digital que se adecúan a sus compromisos multilaterales y a su entorno interno.

Marco Jurídico Internacional

El derecho internacional ha hecho progresos graduales en la aceptación del ciberespacio como un ambiente donde prevalecen las normas esenciales de la Carta de las Naciones Unidas (1945), sobre todo en lo que concierne a soberanía, no intervención y ejercicio legítimo de la fuerza. La Carta, en su Artículo 2(4), prohíbe la utilización de la fuerza contra la independencia

política o integridad territorial de los Estados. Esta cláusula se entiende actualmente de manera amplia, incluyendo así las operaciones cibernéticas que tengan el potencial de generar consecuencias similares a un asalto armado tradicional.

El Artículo 51 también reconoce el derecho inherente a la autodefensa, un principio que, de acuerdo con los documentos del Grupo de Expertos Gubernamentales (GGE) de la ONU (2013, 2015, 2021), puede ser utilizado en caso de ataques cibernéticos cuya gravedad sea comparable a una agresión armada. La importancia de que los Estados respeten el Derecho Internacional Humanitario (DIH) y los Derechos Humanos, incluso en el entorno digital, es otro punto que estos informes resaltan.

El Convenio de Budapest sobre ciberdelincuencia, establecido en 2001, es el instrumento más relevante en el campo específico de la ciberdelincuencia. Este acuerdo del Consejo de Europa fue confirmado y adoptado por más de 60 naciones, incluyendo Colombia, que lo ratificó mediante la Ley 1928 de 2018 (Congreso de la República de Colombia, 2001/2018). Este convenio se convierte en un modelo a nivel global para combatir los delitos informáticos y fortalecer la seguridad digital.

Además, la UIT (Unión Internacional de Telecomunicaciones) y la OEA (Organización de Estados Americanos) han promovido estructuras de cooperación a nivel regional para potenciar las competencias en ciberseguridad y en recuperación digital. La Estrategia Interamericana de Seguridad Cibernética (Organización de los Estados Americanos O.E.A, 2016) fomenta en América Latina la creación de centros de respuesta ante incidentes cibernéticos (CSIRT) y el fortalecimiento de capacidades tanto legales como técnicas en los países miembros.

Estos instrumentos globales funcionan como un marco de referencia para la formulación de políticas nacionales, incorporando principios como la cooperación, la atribución, la proporcionalidad y la responsabilidad del Estado, que son fundamentales para el desarrollo de doctrinas militares adecuadas a las circunstancias digitales.

Marco Jurídico Nacional de Colombia

Colombia ha progresado de manera notable en la creación de una estructura jurídica y estratégica enfocada en proteger el dominio cibernético, la resiliencia digital y la salvaguarda de los activos esenciales del Estado. Estas normas son la respuesta a los compromisos internacionales y a las exigencias internas que surgen de la digitalización en expansión de la seguridad nacional.

Constitución Política de 1991

Las bases del marco jurídico en relación con los derechos digitales, la defensa y la seguridad están definidas en la Constitución colombiana (Asamblea Nacional Constituyente, 1991), así:

Según su artículo 2, los objetivos fundamentales del Estado son preservar la integridad nacional y los bienes de sus ciudadanos, garantizando su seguridad.

El artículo 15 establece el derecho a la privacidad y al hábeas data, fundamentales para la protección de datos digitales.

El artículo 189, numeral 4, otorga al presidente la autoridad para preservar el orden público y la seguridad nacional, lo que incluye el ámbito cibernético.

De igual manera, el artículo 217 define las responsabilidades de las Fuerzas Militares, enfocadas en proteger la independencia, la soberanía y la integridad territorial. Estas obligaciones se han ampliado en la era digital al ciberespacio como una extensión del dominio de defensa multidimensional.

De igual manera, el artículo 217 establece las responsabilidades de las Fuerzas Militares, enfocadas en proteger la independencia, la soberanía y la integridad territorial. Estas obligaciones se han ampliado hoy en día al ciberespacio como una extensión del dominio de defensa multidimensional (Asamblea Nacional Constituyente, 1991).

Legislación Sobre Ciberdelincuencia y Seguridad Digital

Ley 1273 del 2009: Introduce un nuevo bien jurídico denominado "protección de datos e información", que engloba los delitos informáticos como el acceso abusivo, la avería de sistemas informáticos, la interceptación ilegal y el uso de software malicioso, (Congreso de la República de Colombia, 2009).

Ley 1928 de 2018: Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", suscrito en Budapest el 23 de noviembre de 2001. Esta ley ratifica el marco global para la tipificación penal de delitos informáticos y fortalece la cooperación internacional en la materia (Congreso de la República de Colombia, 2001/2018).

Ley 1581 de 2012: Determina principios de finalidad, libertad, seguridad y legalidad que son aplicables para proteger los datos personales, (Congreso de la República de Colombia, 2012).

Ley 1621 de inteligencia y contrainteligencia: establece las pautas legales para compilar información estratégica, que pueden ser utilizadas también en el ámbito cibernético y de ciberinteligencia. (Congreso de la República de Colombia, 2013).

Políticas y Estrategias Nacionales

La Política Nacional de Seguridad Digital (CONPES 3854) propia del (Departamento Nacional de Planeación, 2016) en donde la estrategia inicial que considera la seguridad digital como un asunto de Estado, promoviendo el trabajo conjunto entre entidades y la capacidad para recuperarse después de ser atacadas cibernéticamente. La Política Nacional de Confianza y Seguridad Digital, que fue establecida en el CONPES 3995 del año 2020, tiene como objetivo fortalecer las habilidades de ciberdefensa, ciberseguridad y Ciberinteligencia (Departamento Nacional de Planeación, 2016). Para lograrlo, fomente la formación de personal especializado y la cooperación entre los sectores público y privado.

El Comando Conjunto Cibernético (CCOC) se constituye, de algún modo, como un componente operativo de las Fuerzas Militares mediante el Decreto 1414 de 2017. Su objetivo es proteger infraestructuras críticas y coordinar la reacción ante sucesos cibernéticos. La digitalización segura es vista como un pilar transversal del desarrollo en el Plan Nacional de Desarrollo para 2022 a 2026, enfatizando que la gobernanza digital debe ser fortalecida y las infraestructuras estratégicas resguardadas.

Marco Doctrinal Militar

La doctrina Damasco, que ha sido incorporada por el Ejército Nacional de Colombia, describe el ciberespacio como un entorno operacional novedoso que se integra dentro de las operaciones en varios dominios y de niveles estratégicos conjuntos. Esta doctrina incentiva el desarrollo de capacidades en ciberdefensa, resiliencia digital y Ciberinteligencia, respetando las normativas nacionales y los tratados internacionales (Centro de Doctrina del Ejército, 2020).

Las normas internacionales y nacionales aseveran que es fundamental encontrar un equilibrio entre el acato a los derechos humanos digitales, la cooperación global y la protección de la seguridad nacional para establecer normas sobre ciberdefensa y guerra cibernética. Encaminados sobre los lineamientos de la OEA, los principios de la ONU y las normas del Pacto de Budapest, Colombia venido presentando una evolución en la creación de un sistema normativo integral que respalda la doctrina militar actual.

Pese al reto actual, es conseguir que la ley se ajuste a los avances tecnológicos, como la inteligencia artificial en el sector militar, y robustecer las estructuras de gobernabilidad del ciberespacio para certificar una seguridad digital sólida, soberana y ética (Pardo, J. M., 2024).

Tabla 3

Marco Normativo Internacional y Nacional

Nivel	Instrumento Normativo	Año	Organismo Emisor	Aporte Principal
Internacional	Carta de las Naciones Unidas	1945	ONU	Establece los principios de soberanía, no intervención y uso legítimo de la fuerza, aplicables al ciberespacio.
Internacional	Convenio de Budapest sobre Ciberdelincuencia	2001	Consejo de Europa	Marco global para tipificación penal de delitos informáticos y cooperación internacional.

Internacional	Informes del Grupo de Expertos Gubernamentales (GGE)	2013–2021	Naciones Unidas	Reconoce la aplicación del Derecho Internacional y del DIH a las operaciones cibernéticas.
Internacional	Estrategia Interamericana de Seguridad Cibernética	2016	OEA	Fomenta políticas nacionales, creación de CSIRT y cooperación regional en ciberseguridad.
Internacional	Guías de la UIT sobre Ciberseguridad Global	2019	Unión Internacional de Telecomunicaciones	Promueve la gobernanza digital y la protección de infraestructuras críticas.
Nacional (Colombia)	Constitución Política de Colombia	1991	Asamblea Nacional Constituyente	Define principios de soberanía, defensa y protección de derechos digitales (Art. 2, 15, 217).
Nacional	Ley 1273 de 2009	2009	Congreso de la República	Crea el bien jurídico de "protección de la información y de los datos" y tipifica delitos informáticos.
Nacional	Ley 1928 de 2018	2018	Congreso de la República	Ratifica el Convenio de Budapest, fortaleciendo la cooperación internacional.
Nacional	Ley 1273 de 2009	2009	Congreso de la República	Regula la protección de datos personales y establece principios de tratamiento digital.
Nacional	Ley 1581 de 2012	2012	Congreso de la República	Regula y dictan disposiciones generales para la protección de datos personales.
Nacional	Ley 1621 de 2013	2013	Congreso de la República	Define el marco de la inteligencia y contrainteligencia, incluyendo operaciones digitales.
Nacional	CONPES 3854	2016	Departamento Nacional de Planeación	Primera Política Nacional de Seguridad Digital, promueve coordinación interinstitucional.
Nacional	Decreto 1414	2017	Presidencia de la República	Constituye al Comando Conjunto Cibernético (CCOC) como un organismo encargado de la defensa en el ámbito cibernético.
Nacional	Doctrina Damasco	2019 (actualizada 2023)	Fuerzas Militares de Colombia	Reconoce y/o acepta el ciberespacio como un dominio operativo cuando se incorporan operaciones de múltiples dominios.
Nacional	CONPES 3995	2020	Departamento Nacional de Planeación	Establece la Política de Confianza y Seguridad Digital, fortaleciendo ciberdefensa y Ciberinteligencia.

Nota. Los apartados presentados integran el marco normativo, constitucional y doctrinal que regula la seguridad digital y el ciberespacio, desde los instrumentos internacionales hasta la legislación y políticas adoptadas en Colombia. Adaptada de "*Marco Legal Implementado dentro de la Monografía"*, (2025), (Martínez R.D., 2025).

Marco Histórico

En términos generales, la historia de la guerra ha colaborado en el ajuste de los ejércitos a nivel conceptual y tecnológico, ante los cambios que tienen lugar en el ámbito político, social y científico. La doctrina militar ha experimentado transformaciones a lo largo de la historia, desde las disputas convencionales en los siglos XIX y XX hasta las confrontaciones híbridas y digitales en el siglo XXI, como respuesta a los cambios en la naturaleza del poder y en las técnicas de enfrentamiento. En este proceso, el surgimiento de la guerra cibernética es una de las etapas más disruptivas, ya que desafiaba las ideas convencionales sobre soberanía, territorio y uso legítimo de la fuerza. Se presenta un panorama en el que las luchas ocurren en lugares invisibles y sus consecuencias superan los confines físicos.

De la Guerra Convencional a la Guerra Digital

La doctrina militar se basaba en los principios de la guerra convencional, que abarcaban el dominio territorial, la preeminencia del fuego y la jerarquía en las fuerzas armadas. Esto sucedió a lo largo de un largo período en el siglo XX. No obstante, en la última parte del siglo XX, a causa de la revolución informática y de la difusión mundial de las tecnologías informáticas, aparecieron nuevos tipos de conflictos que se extendieron más allá de los campos de combate convencionales. El ciberespacio se ha convertido en un entorno operativo clave donde la manipulación de información, el espionaje y el sabotaje han llegado a ser herramientas de poder.

Señalaron un punto de inflexión los ataques a Estonia en 2007, el sabotaje de las instalaciones nucleares de Irán usando Stuxnet en 2010 y las operaciones digitales realizadas

durante los enfrentamientos entre Ucrania y Rusia (2014;2022). Estos sucesos evidenciaron que los ciberataques tienen la capacidad de interrumpir infraestructuras esenciales, modificar procesos políticos y provocar efectos estratégicos similares a los de un ataque armado convencional (Rodríguez, P. A., 2025).

Evolución Doctrinal Global y Surgimiento Del Ciberpoder

La doctrina militar sufrió un cambio significativo debido a la aparición del ciberespacio como un nuevo ámbito de guerra. El término "ciberpoder", que hace referencia a la capacidad de un Estado para ejercer poder a través de medios digitales con el objetivo de persuadir, disuadir o coaccionar, fue introducido por autores como (Libicki, M. C., 2009) y (Nye, J. S., 2010). Esta visión amplía la comprensión del poder estratégico más allá de lo físico, al reconocer que la interconexión digital conlleva una vulnerabilidad e influencia. Algunas de las fuerzas militares más importantes de Estados Unidos, Rusia, China y ciertos integrantes de la OTAN comenzaron a incluir habilidades cibernéticas, tanto ofensivas como defensivas, en sus doctrinas desde el 2010 (Pessino, 2017). Para tal propósito, se han establecido estructuras como los Cyber Commands y marcos regulatorios para las operaciones en el ciberespacio. Este procedimiento reforzó la idea de que el dominio cibernético debería ser visto como un campo funcional autónomo, con sus propias estrategias, principios y tácticas.

Respuesta Regional Latinoamericana

En Latinoamérica, el avance de las políticas de ciberdefensa y ciberseguridad ha sido más lento. Por medio de informes como el del 2021, la (Organización de los Estados Americanos

O.E.A, 2016) destacó la importancia de adquirir competencias para fortalecer las capacidades estatales ante el crecimiento de los ataques cibernéticos. Brasil, Chile y Colombia, entre otros países, comenzaron a poner en práctica estrategias nacionales para preservar las infraestructuras fundamentales, formar recursos humanos especializados y fomentar la cooperación internacional. Sin embargo, Dunn Cavelty y Wenger (2020) señalan que las doctrinas militares latinoamericanas han integrado la ciberdefensa como un componente secundario de estructuras existentes en lugar de establecer un modelo doctrinal autónomo capaz de entender cabalmente lo específico del ámbito cibernético.

Desarrollo Histórico en Colombia

El Comando Conjunto Cibernético (CCOC), institución encargada de coordinar las respuestas y los protocolos de ciberdefensa frente a incidentes digitales, se desarrolló en 2011 en Colombia, año en el cual la defensa se digitalizó. Este proceso se fortaleció gracias a la Política Nacional de Seguridad Digital, lanzada en 2016, y al Documento CONPES 3995, publicado en 2020. Ambos establecieron un marco estratégico para proteger la infraestructura digital y fomentar una cultura de resiliencia digital. En el lapso de tiempo entre 2020 y 2025, Colombia ha tomado parte en ejercicios de ciberdefensa a nivel internacional, ha incluido conceptos de Ciberinteligencia en sus procedimientos operativos e iniciado la incorporación del dominio cibernético en su doctrina militar. Sin embargo, el país tiene el reto de elaborar una doctrina integral que una los elementos técnicos, éticos y legales necesarios para encarar amenazas asimétricas en el ciberespacio (Suarez, J. S., 2023).

Crisis Conceptual de la Doctrina Militar Contemporánea

La doctrina militar contemporánea enfrenta una crisis de ideas debido al aumento de la guerra cibernética y la incorporación de inteligencia artificial en el ámbito militar. Esta circunstancia requiere una evaluación exhaustiva de los principios convencionales del empleo de la fuerza, así como una redefinición de las nociones de responsabilidad ética, soberanía y conflicto. La aplicación del Derecho Internacional Humanitario se ve tensionada debido a la rapidez y el anonimato de las operaciones digitales, además de su naturaleza transnacional. Por lo tanto, es necesario entrenar a los militares en competencias éticas y técnicas más avanzadas.

Para comprender este proceso, la investigación actual se fundamenta en tres ejes teóricos primordiales que explican de qué manera la guerra cibernética impacta la doctrina militar. El primero es la guerra híbrida; Hoffman (2009) argumenta que las guerras híbridas combinan tácticas convencionales y no convencionales, incluidas las de ciberespacio, lo cual crea situaciones de conflicto con varios aspectos. Clarke y Knake (2010) añaden que la guerra cibernética es una de estas tácticas, incluyendo espionaje, sabotaje y distorsión de la información.

En segundo lugar, Mahnken (2011) destaca también la importancia de combinar acciones en el aire, el mar, la tierra, el ciberespacio y el espacio. Healey (2024) categoriza las operaciones cibernéticas según su ubicación, tiempo y finalidad; por otro lado, Dunn Cavelty y Wenger (2020) advierten sobre la falta de doctrinas independientes en democracias emergentes.

En tercer lugar, según (Nye, J. S., 2010) y (Libicki, M. C., 2009), el término "ciberpoder" se refiere a la capacidad del Estado de ampliar su influencia mediante el ciberespacio. Mientras que Waxman (2012) argumenta sobre cuestiones legales relacionadas con la naturaleza de las

operaciones cibernéticas y su condición como "ataques armados", es por ello que se advierte sobre los riesgos de depender excesivamente de la tecnología a escala global y del debilitamiento de la soberanía (Timmers 2019, como se citó en Rojo, 2021).

Proyección Histórica

La síntesis de estos avances indica que la doctrina militar tiene que avanzar hacia un modelo integrado y dinámico, que incluye marcos legales adaptables, tecnologías emergentes y métodos concretos de capacitación. Esto implica que, para Colombia, la estrategia militar debe pasar de una doctrina centrada en los dominios físicos convencionales a una visión multifacética, donde el ciberespacio y la ciberinteligencia se vuelven esenciales para la defensa del país. El desafío de hoy en día es desarrollar una doctrina cibernética soberana que tenga la capacidad de integrarse con los aliados internacionales y, al mismo tiempo, se ajuste a los principios del Derecho Internacional Humanitario. La cuestión es garantizar una respuesta ética y efectiva frente a los peligros ocultos del mundo digital de hoy.

Metodología

Con el propósito de garantizar la transparencia y la trazabilidad en cada fase del proceso, se realizó el presente estudio con un enfoque sistemático de revisión bibliográfica (Booth, A., Sutton, A., & Papaioannou, D., 2016). La guía PRISMA 2020 fue la referencia empleada, debido a que este tipo de diseño es apropiado para los fines del estudio, pues la meta es determinar, valorar y sintetizar la producción académica y los documentos institucionales que analizan el vínculo entre la asignatura de guerra cibernética y doctrina militar en Colombia durante el periodo de 2020 a 2025 (Linares Espinós et al., 2018).

Se utilizó el modelo PICOC para formular la pregunta de investigación, lo que permitió determinar con precisión los criterios de búsqueda. Por lo tanto, los documentos oficiales y las investigaciones académicas asociadas con las Fuerzas Militares de Colombia se consideran como población. En cuanto a la intervención, se centró en las maniobras y actividades relacionadas con la guerra cibernética, la ciberdefensa y la ciberinteligencia. El propósito de la comparación fue identificar las alteraciones y cambios en la doctrina militar de Colombia, especialmente en la Doctrina Damasco, y se llevó a cabo con doctrinas militares previas o con relevantes experiencias internacionales. Por último, el análisis se limitó al país dentro del período de 2020 a 2025. Pregunta de investigación (PICOC).

La interrogante de investigación se realiza utilizando los estándares PICOC, que posibilitan la definición precisa del enfoque de búsqueda y de los criterios de inclusión/exclusión:

Población (P): Doctrina militar colombiana y planes de estudio de las Fuerzas Militares.

Intervención (I): Sugerencias para incorporar la guerra cibernética como materia o elemento del plan de estudios.

Comparación (C): Los planes de formación militar de otros países que han incluido este asunto.

Resultados (O): Normas del currículo, estructura de una asignatura, capacidades a desarrollar.

Contexto (C): Colombia, entre 2020 y 2025.

La estrategia de búsqueda abarcó una búsqueda minuciosa en bases de datos académicos tales como: Dialnet, Google Scholar, Scopus, SciELO y Web of Science. Además, se sumó a esta búsqueda el uso de repositorios institucionales del Ministerio de Defensa, la Escuela Superior de Guerra y el (Departamento Nacional de Planeación, 2016). Se emplearon agrupaciones de palabras clave y operadores booleanos en español e inglés, como "guerra cibernética", "ciberdefensa", "doctrina militar", "cyberwar" y "Colombia". La estrategia de búsqueda abarcó una búsqueda minuciosa en bases de datos académicos tales como: Dialnet, Google Scholar, Scopus, SciELO y Web of Science.

El procedimiento de selección se llevó a cabo siguiendo las fases del diagrama PRISMA 2020. Se detectaron 775 registros al principio, de los cuales se descartaron 145 que estaban duplicados. Después, se revisaron 630 títulos y resúmenes, de los cuales se eliminaron 480 por no cumplir con los criterios de inclusión. Finalmente, se revisaron 150 textos completos y de ellos, 47 estudios fueron incorporados en el análisis cualitativo. Los estudios que fueron

preseleccionados pasaron a una evaluación más completa del texto completo para comprobar su pertinencia con respecto a los criterios de inclusión y exclusión previamente establecidos. Solo aquellos documentos que cumplieron con todos los criterios definidos fueron incluidos en la síntesis final.

Condiciones Para Ser Elegible

Inclusión

Investigaciones publicadas entre los años 2020 y 2025.

Idiomas: inglés y español.

Tesis académicas, informes oficiales, informes técnicos y artículos revisados por pares.

Investigaciones enfocadas en la doctrina militar, la guerra cibernética o la ciberdefensa en Colombia.

Exclusión

Publicaciones que fueron hechas antes de 2020.

Documentos sin texto completo.

Prensa o literatura de divulgación sin análisis de carácter académico.

Estudios o ilustraciones alusivas a la ciberseguridad solamente en el ámbito privado, sin incluir mecanismos doctrinales o militares.

Fuentes de Información y Estrategia de Búsqueda

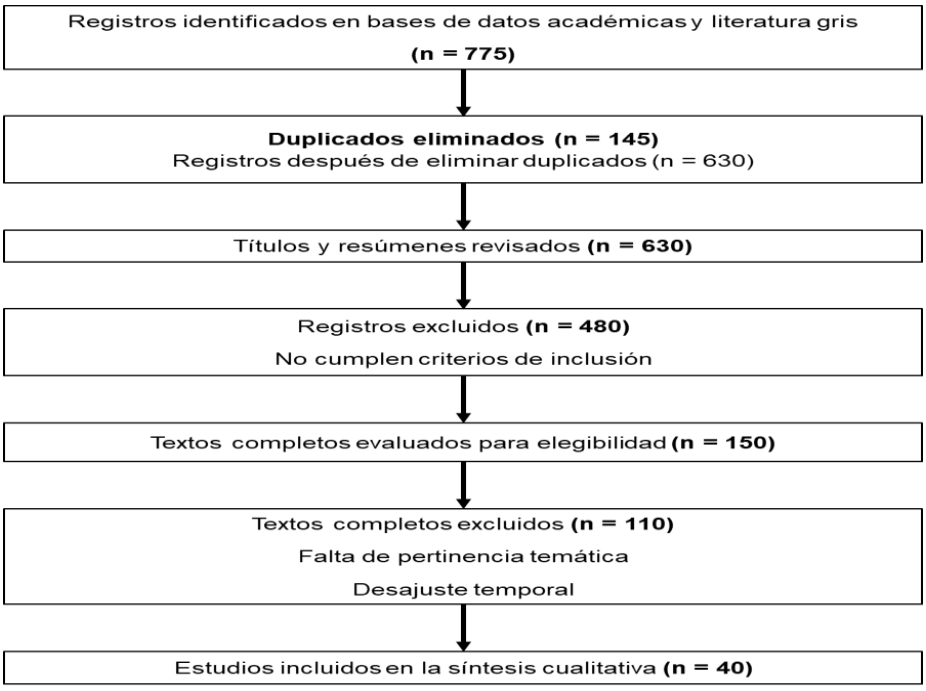
Para la estrategia de búsqueda, se realizará mediante Google Scholar, Scopus, Web of Science, SciELO y Dialnet, de igual manera se emplearán repositorios institucionales del (Ministerio de Defensa, Escuela Superior de Guerra, DNP). Ejemplo de cadenas de búsqueda: "Colombia" Y ("guerra cibernética" o "cyberwar" o "ciberdefensa") y ("doctrina militar" o "Fuerzas Militares") y 2020-2025, "Doctrina Damasco" y "Colombia" y "ciberseguridad".

Para ilustrar el procedimiento de identificación, selección y síntesis de estudios, se realiza un diseño con la metodología del diagrama PRISMA 2020. Este método presenta esquemáticamente el número de registros que se identifican durante la búsqueda inicial, cuántas publicaciones fueron descartadas en cada fase y qué estudios integraron la síntesis final. El análisis se complementa con el diagrama, que proporciona una representación precisa del proceso metodológico utilizado en la investigación.

El proceso de búsqueda sistemática hizo posible, al principio, detectar 775 registros que procedían de literatura gris y bases de datos académicos. Después de eliminar 145 duplicados, se examinó un total de 630 títulos y resúmenes. Se descartaron 480 porque no cumplieron con los criterios de inclusión. Después, se revisaron 150 textos completos; sin embargo, se descartaron 110 por no ser relevantes temáticamente, por desajuste temporal o baja calidad metodológica. En última instancia, para la discusión sobre el impacto de la guerra cibernética en la doctrina militar de Colombia y para el análisis cualitativo, se incluyeron 40 estudios en el corpus de análisis.

Figura 4

Diagrama PRISMA 2020-Revision Sistemática



Nota. Proceso sistemático de identificación, cribado, evaluación de elegibilidad e inclusión de la guerra cibernética como asignatura en la doctrina militar de Colombia. Adaptada de *"Diagrama PRISMA 2020"* [Imagen] (Martínez R.D., 2025).

Se elabora una matriz en Excel para extraer datos, lo que posibilitó la captura uniforme de elementos clave de cada publicación, como el autor, el año, la finalidad, el método utilizado, los hallazgos más importantes y las contribuciones a la doctrina militar de Colombia. La información fue analizada y organizada por medio de una fusión narrativa y temática, centrada en tres ejes fundamentales: el progreso doctrinal de las Fuerzas Militares, la mejora de capacidades en ciberseguridad y los retos jurídicos y políticos relacionados con el ciberespacio como un nuevo dominio operativo.

Posibilitando aterrizar la calidad metodológica de los estudios escogidos, en los que se utilizó la herramienta CASP (Critical Appraisal Skills Programme) para evaluar un grupo de preguntas estandarizadas con el fin de determinar si la evidencia existente es válida, rigurosa y relevante. Los resultados de esta evaluación se consolidaron en una matriz que posibilitó determinar cuán sólidas eran las conclusiones de cada publicación y, por ende, respaldar la confiabilidad de los hallazgos de este análisis.

Evaluación de Calidad (CASP)

Para evaluar la calidad de los estudios incluidos, se empleará el programa CASP (Critical Appraisal Skills Programme), que consta de diez elementos. Esta herramienta posibilita el estudio de la credibilidad de los resultados, la aplicabilidad en términos prácticos, la claridad de las metas y la rigurosidad del método. Exhibiendo una matriz CASP (Tabla 4) que presentará los resultados de la evaluación de cada investigación, acompañada de una justificación concisa.

Tabla 4

Matriz de Evaluación de Calidad (CASP)

Estudio	1. Claridad del objetivo	2. Apropiación del método cualitativo	3. Diseño adecuado para la pregunta	4. Descripción de la selección de fuentes/participantes	5. Reflexividad del investigador	6. Recogida de datos adecuada	7. Consideraciones éticas	8. Análisis riguroso y creíble	9. Presentación clara de resultados	10. Aplicabilidad práctica / transferencia
Peña Suárez, J.S. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. Perspectivas en Inteligencia.	Sí — el objetivo de revisar los desafíos está declarado	Sí — utilizan análisis documental cualitativo.	Sí — diseño consistente para diagnosticar desafíos institucionales.	No claro — menciona fuentes como libros y artículos, pero no detalla	No — no hay reflexión explícita sobre la posición del autor ni posibles sesgos.	Sí — se consultan múltiples fuentes académicas e	No claro — no se menciona aprobación ética (no hallado), aunque	Sí — el análisis es presentado con argumentación, citas y ejemplos.	Estudio	Sí — tiene implicaciones para política, doctrina militar y capacidades institucionales.

15(24), 333-359. http:// doi.org/10.47961/2145194X.628	clarame nte.			criterios de inclusión/exclusión de forma rigurosa.		instituci onales.	al ser documental puede no aplicars e tanto.			
Pardo, J. M. (2024). Normatividad para la protección cibernética de la infraestructura crítica en Colombia. Ciberespacio, Tecnología e Innovación, 3(5), 7-32.	Sí — el objetivo de revisar la normativi dad está claro.	Sí — enfoque documental con matriz DOFA.	Sí — el diseño examina las regulaciones, decretos y leyes pertinentes.	Sí — aclara que examina las normas nacionales y las fuentes identificadas	No claro — no parece discutirse la manera en que el investigador o la institución pueden afectar la interpretación.	Sí — hay datos suficientes (decretos, normas, publicaciones oficiales)	No está claro — no se señala la aprobación ética, hay escasa reflexividad.	Sí — el análisis DOFA proporciona una credibilidad adecuada y una presentación equilibrada de las fortalezas y debilidades.	Sí — resultados bien presentados, con sugerencias prácticas.	Sí — muy aplicable para formuladores de política, fuerza militar, infraestructura crítica.
Rodríguez, P. A. (2025) «Operaciones cibernéticas en el nivel operacional de la guerra: lecciones del conflicto entre Rusia y Ucrania», Revista Ciberespacio, Tecnología e Innovación, 4(7), pp. 15–40. doi: 10.25062/2955-0270.4942.	Sí — busca extraer lecciones operacionales aplicables, objetivo bien planteado.	Sí — es un método cualitativo que se basa en el examen de documentos y el análisis de casos.	Sí — un diseño adecuado para lecciones externas o preguntas comparativas que se aplican en el ámbito militar.	No claro — se se hace referencia al conflicto entre Ucrania y Rusia como un caso, pero no está del todo claro cómo se selecciona n los ejemplos específicos.	No — no se evalúa explícitamente la posición del autor o su posible parcialidad al elegir fuentes.	Sí — consulte artículos recientes acerca de las operaciones, así como informes oficiales y literatura especializada.	No — no se menciona revisión ética; al ser un análisis secundario podría no requerirse, pero no se hace explícito.	Sí — razonamiento claro, uso de evidencia contrastada, conclusiones basadas en los datos analizados.	Sí — estructura clara, con lecciones explícitas para doctrina y planeamiento militar.	Sí — útil para doctrinas militares que buscan adaptarse a nuevos dominios de guerra; transferible.
Rodríguez, A. G. (2015). Cibernética en la guerra contemporánea: definición de nuevos escenarios estratégicos y operacionales. En la revista de Seguridad y Defensa, 10(20), se encuentran los números 117 a 131.	Sí — establece lo que se entiende por cibergue rra/ciber nética en contexto s nuevos.	Sí — de nuevo analítico / descriptivo y documental.	Sí — diseño teórico-estratégico se encuentra en línea de cómo se redefine el panorama militar. r.	No claro — se citan fuentes documentales, pero no se explica con claridad el criterio de selección.	No claro — poco discurso sobre influjos del autor o institucionalidad del estudio.	Sí — suficientes ejemplos conceptuales y teóricos para sustentar definiciones.	No claro — reflexión ética mínima.	Sí — el análisis conceptual es consistente, argumentado.	Sí — los resultados presentados con claridad conceptual, escenarios estratégicos identificados.	Sí — útil para quienes diseñan doctrinas, entrenamiento militar, políticas de estrategia.

Nota. Tabla matriz de la respectiva evaluación de Calidad (CASP) generada para los estudios seleccionados. Adaptada de *"CASP (Critical Appraisal Skills Programme)"* (2025), (Martínez R.D., 2025).

Desarrollo del Estudio Monográfico

Este capítulo presenta el análisis y la discusión de los hallazgos de la revisión sistemática realizada bajo la metodología PRISMA 2020, cuya calidad fue evaluada mediante la herramienta CASP (Tabla 4). Los resultados se organizan y discuten en función de cada uno de los objetivos específicos del estudio, sirviendo como base fundamental para la propuesta curricular desarrollada en el ítem de “Resultados”.

Análisis en Función al Objetivo Específico 1: Identificar la Consecuencia de la Guerra Cibernética en la Doctrina Militar de Colombia.

La revisión sistemática permitió identificar que la guerra cibernética ha tenido un impacto profundo y multifacético en la doctrina militar colombiana, forzando una evolución desde los paradigmas convencionales hacia la incorporación del ciberespacio como un dominio operativo más. Este hallazgo es consistente en estudios como el de Peña Suárez (2023), el cual, según la evaluación CASP, presenta un análisis riguroso y creíble, así como una alta aplicabilidad práctica. El estudio destaca cómo las Fuerzas Militares colombianas enfrentan un "desafío en la era digital" que requiere una actualización doctrinal urgente para contrarrestar amenazas híbridas.

La Matriz CASP (Tabla 4) revela que investigaciones como la de Rodríguez (2025), calificada con alta claridad en sus objetivos y rigor analítico, proporcionan lecciones operacionales cruciales a partir de conflictos como el de Ucrania-Rusia. Estas lecciones subrayan la necesidad de que la doctrina colombiana desarrolle tácticas defensivas innovadoras, como la "defensa en profundidad" y el fortalecimiento en la defensa de infraestructuras críticas. La

discusión aquí se centra en cómo estos conceptos, validados por la evidencia de calidad, deben reflejarse en contextos operativos contemporáneos colombianos, superando el enfoque reactivo y fragmentado que aún persiste.

En síntesis, el análisis de la literatura de calidad seleccionada confirma que la principal consecuencia de la guerra cibernética es la necesidad de una transformación doctrinal proactiva y adaptativa, que integre de forma explícita principios, protocolos y tácticas para el dominio cibernético.

Análisis en Función al Objetivo Específico 2: Establecer Las Nociones Doctrinales, Pedagógicas y Tecnológicas Para la Inclusión de la Guerra Cibernética.

El análisis de los estudios incluidos, particularmente aquellos con alta puntuación en la dimensión de "Aplicabilidad práctica" de la Matriz CASP (Tabla 4), permitió establecer un triplete de nociones fundamentales que respaldan la inclusión de la asignatura.

Nociones Doctrinales

El estudio de Realpe Díaz (2019), aunque anterior al rango 2020-2025, es citado consistentemente en la literatura más reciente como base fundamental. Trabajos como el de Pardo (2024), que según CASP presenta un diseño adecuado y un análisis riguroso, argumentan que la normatividad nacional (ej. CONPES 3995, Doctrina Damasco) ya sienta las bases doctrinales para reconocer el ciberespacio. La discusión se centra en cómo estas bases deben traducirse en un mandato curricular explícito.

Nociones Pedagógicas

La evaluación CASP destaca que investigaciones como las de Rivera Alturo & Hernández García (2023) abordan de manera clara y con datos suficientes la necesidad de enfoques de aprendizaje activo. Se discute cómo sus hallazgos respaldan la implementación de metodologías como el Aprendizaje Basado en Problemas (ABP) y la simulación, cruciales para desarrollar el razonamiento estratégico en entornos digitales.

Nociones Tecnológicas

Los informes de Fortinet et al. (2024) y el análisis de Gamboa (2023) cuya claridad y aplicabilidad son evidentes proveen la justificación tecnológica. Se discute cómo la evidencia sobre el volumen y sofisticación de ciberataques exige que el entrenamiento militar incluya laboratorios de ciberseguridad y herramientas de simulación, no como un lujo, sino como una necesidad operativa.

La discusión consolida que estas tres nociones están intrínsecamente ligadas y son indivisibles para una propuesta de formación coherente con las políticas nacionales de defensa y educación.

Análisis en Función al Objetivo Específico 3: Clasificar y Sistematizar Las Fuentes Para Establecer un Marco de Referencia Curricular

El proceso de revisión sistemática y la aplicación de los criterios CASP permitieron la selección y clasificación rigurosa de 47 estudios que constituyen el corpus de esta investigación. La Matriz CASP (Tabla 4) fue instrumental en este objetivo, al permitir discriminar entre la

abundante literatura disponible y seleccionar solo aquella que cumplía con estándares de calidad metodológica, relevancia y aplicabilidad. Por ejemplo, se identificaron y clasificaron:

Fuentes Doctrinales

Documentos oficiales como la Doctrina Damasco (CEDOE, 2020) y los CONPES, cuya autoridad y relevancia son incuestionables para el contexto colombiano.

Fuentes Académicas

Artículos de revistas indexadas como la Revista Científica General José María Córdova y Perspectivas en Inteligencia, que, como muestra la evaluación CASP, suelen presentar objetivos claros y análisis rigurosos.

Fuentes Científicas y Técnicas

Informes globales (Foro Económico Mundial, Fortinet) que proporcionan datos duros y tendencias, enriqueciendo el marco de referencia con una perspectiva internacional. La discusión se centra en cómo esta sistematización, lejos de ser un mero ejercicio bibliográfico, construyó un marco de referencia sólido y multifacético. Este marco no solo apoya la propuesta curricular, sino que también asegura que esta esté alineada con la evidencia más actual y confiable, cerrando la brecha entre la teoría académica, la doctrina institucional y las necesidades operativas prácticas.

Resultados

Para la incorporación de la asignatura de guerra cibernética en la doctrina militar colombiana se contemplan fundamentos elementales para su inclusión como asignatura en la actualización curricular.

El Alumno de Las Escuelas de Formación Como Agente Transformador en la Era Cibernética.

En el contexto actual de la educación militar, los alumnos de las Escuelas de Formación Militar (EMSIC - EMSUB) se transforman en una parte indispensable para mejorar la capacidad defensiva del Estado. Incorporar la asignatura de guerra cibernética en la doctrina militar colombiana es crucial; no solamente supera el entrenamiento convencional, sino que además potencia las habilidades digitales, tácticas y cognitivas que fortalecen la defensa del país. La ciberdefensa busca promover competencias ofensivas y defensivas en el ámbito cibernético; asimismo, es un elemento que engloba todos los campos de la formación militar.

La educación militar, al incluir la asignatura de guerra cibernética en su plan de estudios, se ve como una inversión estratégica para el país, no únicamente con el objetivo de formar a oficiales y suboficiales que puedan afrontar los desafíos tecnológicos y geopolíticos actuales. Este procedimiento potencia la calidad de la educación al impulsar el pensamiento crítico, la capacidad para decidir y la innovación en entornos digitales. Para salvar a la nación, es esencial que la educación militar de hoy en día trascienda las visiones tácticas y estratégicas en el ciberespacio y el aprendizaje digital.

Por lo tanto, el objetivo de formar a los expertos del Ejército Nacional en ciberdefensa es fomentar habilidades como la ética, la estrategia y la tecnología, así como educar líderes dinámicos que tengan la capacidad de prevenir, disminuir y afrontar las amenazas en el ámbito cibernético que representan un peligro para la soberanía digital del país. Por lo tanto, la capacitación y la formación militar son fundamentales para alcanzar como resultado la seguridad nacional.

Fundamentos Doctrinales

La doctrina militar actual reconoce varios ámbitos de conflicto, y el ciberespacio se ha consolidado como uno de ellos, siendo un campo propio para operaciones tácticas, estratégicas y operacionales. En Colombia, el artículo 217 de la Constitución Política concede a las Fuerzas Militares la capacidad de defender la independencia, la integridad territorial y el orden constitucional; esto comprende adicionalmente los dominios tecnológicos y digitales que trascienden lo físico.

El trabajo "Estrategia Militar de Ciberdefensa para las Fuerzas Militares de Colombia frente a las amenazas cibernéticas que suponen las tecnologías disruptivas al 2022", escrito por (Realpe Díaz, 2019), enfatiza la importancia de pensar en la ciberdefensa de forma holística, tomando en cuenta puntos de vista a corto, medio y largo plazo. Esta estrategia sugiere que el ciberespacio se ve como un campo legítimo de defensa, lo cual implica habilidades defensivas, ofensivas y cooperativas a nivel global.

Además, la Escuela Superior de Guerra "General Rafael Reyes Prieto" contempla el concepto de ambiente operacional en su catálogo doctrinal, en el que se incluye explícitamente el

ciberespacio como uno de los temas vinculados a la doctrina militar moderna (Fuerzas Militares de Colombia, 2018).

Estos componentes doctrinales establecieron las bases para aceptar que la guerra cibernética es un fenómeno ya no marginal, sino esencial para las tácticas de defensa y seguridad nacionales; por tanto, su inclusión formal y sistemática en la formación militar está justificada.

Ciberespacio y Conflicto Moderno

El conflicto contemporáneo según (Rodríguez, P. A., 2025) no se limita solamente a lo físico; se desarrolla también en el ámbito digital, donde la manipulación de información, los ataques, la interrupción de las comunicaciones y el sabotaje tecnológico constituyen vectores críticos de agresión tanto estatal como no estatal. Un análisis de operaciones cibernéticas a nivel operacional en la guerra entre Ucrania y Rusia ilustra lecciones que las Fuerzas Militares colombianas pueden aplicar la importancia de prever, de contar con inteligencia, de defenderse en profundidad, de que haya interoperabilidad entre organizaciones y de tener una infraestructura crítica resiliente.

Como rama del conocimiento, la cibernética ayuda a comprender el conflicto digital más allá de la misma tecnología: incluye procesos de toma de decisiones, automatización, intercambio de información, amenazas de vulnerabilidad operativa y el cambio permanente del entorno tecnológico (Rodríguez, A. G., 2015). Se ha recomendado en Colombia que los nuevos contextos operativos y estratégicos se establezcan a partir de esta perspectiva cibernética.

Estas modificaciones admiten que la doctrina militar tiene que incluir de manera explícita ideas tales como ciberdefensa, ciberguerra, resiliencia, actores estatales y no estatales en el

ciberespacio, normas internacionales aplicables, ética y legalidad; ya que el dominio tecnológico presume retos para la operatividad militar y para el derecho internacional humanitario.

Educación Militar y Ciberdefensa

Ya se han integrado aspectos relacionados con la ciberdefensa y la ciberseguridad en los programas de posgrado y diplomados para formación militar en Colombia. La Escuela Superior de Guerra, por ejemplo, brinda diplomados centrados en la ciberdefensa y la ciberseguridad, con módulos que abordan temas como las amenazas contemporáneas, las regulaciones, la colaboración internacional y la capacidad de recuperación ante situaciones adversas en infraestructuras críticas (Escuela Superior de Guerra, 2025).

Además, iniciativas académicas como "Proyecto de formación de oficiales en gerencia tecnológica y diseño de sistemas digitales para la ciberdefensa" estudian las tendencias a escala nacional y proponen modelos educativos que se ajustan a las demandas tecnológicas del futuro. (Cortez, G. M., 2024).

Según investigaciones, la ciberseguridad es un enfoque de aprendizaje especialmente importante en el nivel suboficial (Rivera Alturo, L. M., & Hernández García, S. A., 2023). Esto es porque estos actores tienen un papel directo en la protección operativa y en el establecimiento de políticas técnicas, así como también debido a su necesidad de poseer habilidades específicas para identificar amenazas, aplicar buenas prácticas tecnológicas, manejar incidentes y reaccionar.

Sin embargo, el estudio también revela deficiencias como la falta de materias específicas sobre guerra digital en las carreras militares, una cobertura práctica escasa en los laboratorios, la

necesidad de que los profesores se actualicen y la integración entre teoría doctrinal e implementación operativa.

Propuesta Pedagógica Para su Inclusión Curricular

Se propone el siguiente marco pedagógico con el fin de incorporar la asignatura de guerra cibernética como una materia en la actualización del currículo militar:

Título de la Asignatura

La propuesta sugerida de asignatura es de Guerra Cibernética y Ciberdefensa, la cual está orientada a fortalecer las capacidades estratégicas, operativas y técnicas del personal militar.

Objetivo General de la Asignatura

Capacitar a oficiales y suboficiales para que puedan entender las bases teóricas de la guerra cibernética, detectar vulnerabilidades y amenazas, planear y llevar a cabo operaciones defensivas y cooperativas en el ciberespacio, así como aplicar preceptos doctrinarios, legales y éticos tanto nacionales como internacionales.

Competencias Propuestas

Comprensión doctrinal: Definir los conceptos básicos (ciberguerra, ciberdefensa, ciberespacio y amenazas emergentes), y comprender los principios doctrinales y normativos que sustentan la guerra cibernética en el contexto de la defensa nacional.

Análisis estratégico-operacional: Evaluar conflictos y circunstancias, tanto a nivel global como nacional, así como calcular los riesgos, aplicando técnicas y procedimientos de ciberdefensa en entornos simulados, garantizando la protección de infraestructuras críticas.

Competencias técnicas básicas: Seguridad en redes, criptografía básica, respuesta a incidentes y salvaguarda de infraestructuras críticas.

Normatividad y ética: Estudio acerca de los derechos humanos, las leyes nacionales en términos de defensa y ciberseguridad, así como del derecho internacional humanitario, fomentando la ética, responsabilidad y disciplina cibernética en el ejercicio de la defensa nacional.

Cooperación interinstitucional: Colaboración con el sector privado y entre múltiples naciones, así como coordinación entre civiles y militares y diplomacia cibernética.

Contenidos Sugeridos (Temáticos)

Total, sugerido: 58 horas teóricas / 30 horas prácticas

Tabla 5

Contenidos Temáticos Sugeridos.

Módulo	Temática Principal	Horas Sugeridas
Módulo 1	Fundamentos doctrinales y estratégicos de la guerra cibernética	12 horas teóricas
Módulo 2	Conceptos básicos de ciberseguridad y ciberdefensa militar	10 horas teóricas / 4 horas prácticas

Módulo 3	Amenazas, ataques y vulnerabilidades en entornos militares	8 horas teóricas / 8 horas prácticas
Módulo 4	Tecnologías emergentes aplicadas a la defensa cibernética	10 horas teóricas / 6 horas prácticas
Módulo 5	Simulación de operaciones de guerra cibernética y ejercicios tácticos	6 horas teóricas / 12 horas prácticas
Módulo 6	Marco ético, legal y doctrinal de la ciberdefensa en Colombia	12 horas teóricas

Nota. Distribución temática de fundamentos doctrinales, capacidades operacionales y marcos ético legales para el desarrollo de competencias en guerra cibernética y ciberdefensa militar. Adaptado de *"Ministerio de Defensa Nacional de Colombia, Política de Defensa y Seguridad (2019) y OTAN, Cyber Defence Concept (2020)"*. https://www.mindefensa.gov.co - https://www.nato.int

Metodología de Aprendizaje y Enseñanza

La asignatura se desarrollará bajo un enfoque teórico-práctico, que combine la comprensión conceptual con la aplicación operativa. Se emplearán las siguientes estrategias metodológicas:

Lecciones teóricas, acompañadas de simulaciones, análisis de casos y ejercicios prácticos sobre incidentes reales y operaciones militares cibernéticas.

Uso de laboratorios de ciberseguridad para realizar investigación forense digital, contestar a incidentes y penetración.

Aprendizaje basado en proyectos (ABP) orientado al diseño de estrategias de defensa cibernética.

Puestos de trabajo interdisciplinarios (por ejemplo, la cooperación con organismos civiles u otros sectores militares)

Diversas evaluaciones: exposiciones grupales, estudios de casos, redacción de trabajos y simulacros prácticos orientada al desarrollo progresivo de competencias.

Sistema de Créditos y Ubicación en el Plan Curricular

La materia tiene la opción de ser impartida en los niveles más altos del pregrado militar (tercero o cuarto año) o como fundamento para la especialización, con un porcentaje de horas que incluye clases teóricas y prácticas. Asimismo, puede ser impartida como un módulo necesario en las carreras de ciencias militares, navales y aeronáuticas.

Total, de créditos: 3

Carga horaria total: 88 horas

58 horas teóricas / 30 horas prácticas o de laboratorio

La carga puede ajustarse según las disposiciones institucionales y el reglamento académico.

Sistema de Evaluación

Tabla 6

Propuesta del Sistema de Evaluación.

Actividad Evaluativa	Instrumento	Porcentaje
Simulacros y ejercicios prácticos	Rúbricas de desempeño	30%
Trabajos de investigación o análisis doctrinal	Informe técnico / ensayo	25%
Exámenes teóricos	Prueba escrita	20%
Proyectos aplicados o estrategias de ciberdefensa	Evaluación por proyecto	20%
Participación y compromiso ético	Autoevaluación / coevaluación	5%

Nota. Propuesta de evaluación formativa mediante instrumentos que valoran competencias teóricas, prácticas y éticas en ciberdefensa, garantizando resultados de aprendizaje y el desempeño profesional. Adaptado de *"Maestría en Ciberseguridad y Ciberdefensa"* (2025), Escuela Superior de Guerra. https://esdegue.edu.co/es/maestria-en-ciberseguridad-y-ciberdefensa

Retos y Perspectivas Futuras

Se enfrenta a varios desafíos la incorporación de un curso formal sobre guerra cibernética en la doctrina militar colombiana:

Formación de docentes: falta de maestros con experiencia práctica en conflictos digitales.

Infraestructura tecnológica: Recursos tecnológicos adecuados, laboratorios, redes de seguridad y simuladores.

Resistencia cultural: Algunos enfoques tradicionales podrían no estar dispuestos a admitir que el entorno digital se ha convertido en un campo de batalla legítimo.

Políticas públicas y normas: Es esencial tener leyes claras en lo que respecta a la defensa cibernética, la salvaguarda de los derechos humanos y los acuerdos internacionales (Pacheco, J. A., 2022).

Recursos presupuestarios: Distribución adecuada de los presupuestos para emplear la tecnología, contratar a especialistas y mantener el contenido al día.

Proyección a Futuro

Formar alianzas académicas, tanto a nivel nacional como internacional, para compartir saberes y buenas prácticas.

Crear programas de posgrado en el Ejército que se centren en la guerra cibernética y la inteligencia digital.

Realizar investigaciones permanentes sobre las implicaciones éticas y legales de la tecnología disruptiva y de los nuevos peligros.

Garantizar que el currículo militar sea revisado periódicamente para adaptarse a los rápidos cambios en el entorno tecnológico, lo que asegura no solo la inclusión de la materia, sino además su continua actualización.

Recomendaciones

La investigación efectuada posibilita sugerir varias recomendaciones con el propósito de consolidar la inclusión de la asignatura de guerra cibernética en la doctrina militar colombiana, para asegurar que sea oficialmente incluida como una materia curricular en los programas de capacitación y actualización de las Fuerzas Militares. Estas sugerencias se organizan en tres enfoques estratégicos: doctrinal, pedagógico y tecnológico, que están en línea con los objetivos específicos del trabajo.

Sugerencias doctrinales

Actualizar la Doctrina Militar de Colombia

De acuerdo con las pautas internacionales de defensa en lo que se refiere a la ciberseguridad (Realpe Díaz, 2019), el ciberespacio se incorpora como una quinta área operativa, al igual que los espacios marítimo, terrestre, aéreo y espacial. Esta actualización doctrinal debería verse reflejada en los planos de formación, las normativas tácticas y los manuales de operaciones conjuntas del Comando General de las Fuerzas Militares.

Fortalecer Una Política de Defensa Cibernética en el Ámbito Educativo

Está unificando las normas entre las ramas de la Policía Nacional, el Ejército, la Armada y la Fuerza Aérea en lo referente al avance de las habilidades digitales, la ética cibernética y la administración del conocimiento aplicado a la seguridad del país.

Reforzar la Colaboración Internacional en el Campo de la Doctrina Cibernética

A través de convenios con universidades militares de naciones aliadas, la OEA y centros destacados de ciberdefensa de la OTAN. Con esta colaboración, podremos intercambiar prácticas óptimas, simuladores y conocimientos para crear programas de capacitación actualizados (Organización de los Estados Americanos O.E.A, 2016).

Recomendaciones Pedagógicas

Crear e Implementar la Asignatura "Guerra Cibernética y Ciberdefensa"

Esta materia debe ser una parte esencial de los planes curriculares de educación militar. Por esta misma razón, (Gaitán Rodríguez, 2022) indica que este contenido debe abarcar principios operacionales, doctrinales y éticos, utilizando una estructura modular fundamentada en competencias.

Empleo de Técnicas de Enseñanza y Aprendizaje

Enfoques que incluyen la simulación táctica en contextos virtuales, el aprendizaje fundamentado en problemas y la creación de laboratorios para ciberseguridad. Según (Dunleavy, M., Dede, C., & Mitchell, R., 2008), estas tácticas permiten que se desarrollen habilidades críticas y analíticas en contextos de conflicto digital.

Promover la Formación Permanente de los Instructores y Maestros Militares

Educación permanente en temas vinculados a la ética tecnológica, ciberseguridad, estándares internacionales e inteligencia digital. Según el análisis y criterio de (Rivera Alturo, L. M., & Hernández García, S. A., 2023), esto asegurará que la educación sea relevante y esté en consonancia con los desarrollos doctrinales y tecnológicos.

Integrar la Investigación Aplicada

La investigación se convierte en un eje transversal de la instrucción militar, fomentando iniciativas para innovar en tecnología, simulaciones de defensa digital y evaluaciones de eventos cibernéticos. Así pues, se generará un entorno de aprendizaje enfocado en la resolución de problemas específicos relacionados con la seguridad nacional.

Recomendaciones Tecnológicas y Operativas

Proveer a Las Organizaciones Educativas Militares de Infraestructura Tecnológica Específica

Esto abarca laboratorios de ciberdefensa, redes aisladas para simulaciones y sistemas para capacitación en ataque y defensa. Según (Pacheco, J. A., 2022), estos recursos deben respetar las normativas internacionales y garantizar un ambiente seguro para la educación.

Crear Alianzas Con el Sector Académico y Privado

Alianzas que permitirán desarrollar en conjunto programas de certificación técnica en ciberseguridad, simuladores digitales de guerra y software educativo, con el objetivo de potenciar la capacitación práctica y la posibilidad de conseguir empleo en tecnología militar.

Crear un Sistema de Evaluación Permanente

Evaluación del rendimiento y la efectividad de la asignatura de guerra cibernética mediante indicadores vinculados a la competencia, el desempeño operativo y la implementación del conocimiento en circunstancias reales en materia de seguridad nacional.

Sostenibilidad Presupuestaria e Institucional

Es esencial garantizar la viabilidad de las medidas de educación cibernética, que comprenden el entrenamiento constante, la preservación de la tecnología y la actualización periódica del currículo, bajo la supervisión del Centro de Educación y Doctrina o su equivalente en cada fuerza armada.

Recomendaciones de Proyección Futura

Por último, se sugiere establecer una estrategia nacional de educación en ciberdefensa que integre las etapas de formación civil, militar y policial. Esta articulación posibilitará que la cultura de ciberseguridad en el país se refuerce, que la colaboración entre instituciones aumente y que se impulse el desarrollo de una doctrina de defensa integral ante los peligros del siglo XXI.

Además, se recomienda establecer un Observatorio de Ciberdefensa y Educación Militar, cuya función será la de supervisar las tendencias tecnológicas, examinar los sucesos a nivel mundial y producir conocimiento aplicado para que el currículo se mantenga actualizado de manera constante y para la toma de decisiones estratégicas.

Conclusiones

La incorporación de la asignatura de guerra cibernética en la doctrina militar colombiana supone un reto estratégico, doctrinal y educativo para las Fuerzas Militares en una época en que el ciberespacio se establece como un nuevo dominio operativo. Por lo tanto, se hace evidente la necesidad de renovar los programas de formación militar para incorporar materias enfocadas en el estudio, entendimiento y administración de operaciones en el ámbito digital, asegurando así una defensa completa del Estado y sus infraestructuras esenciales.

Respecto al primer objetivo, que buscaba establecer la manera en que las tecnologías emergentes impactan la doctrina militar colombiana, se encontró que el ciberespacio ha transformado la naturaleza de la guerra moderna. Según (Díaz, M. E., 2019), las tiendas contemporáneas se distinguen por utilizar instrumentos digitales para realizar espionaje, sabotear, desinformar y obstaculizar tecnologías. Dada esta circunstancia, es preciso que la doctrina militar reconozca oficialmente a la ciberguerra como una forma legítima de confrontación en el marco de la planificación estratégica nacional. En consecuencia, se mejora la capacidad de respuesta ante los peligros híbridos que fusionan acciones digitales y convencionales (Gaitán Rodríguez, 2022).

Igualmente, el segundo objetivo específico, que se enfoca en presentar las conclusiones resultantes del análisis realizado, ha evidenciado que la doctrina actual sigue teniendo fallas en cuanto a la capacitación de los militares en ciberdefensa. Aunque la Escuela Superior de Guerra "General Rafael Reyes Prieto" brinda diplomados y programas de especialización, estos no se incluyen sistemáticamente en el currículo básico para instruir a oficiales y suboficiales. Esta investigación respalda la importancia de implementar una asignatura sobre guerra cibernética, que combina conocimientos éticos, técnicos y teóricos, y que promueve habilidades en

colaboración entre instituciones, resiliencia tecnológica, evaluación de riesgos y seguridad digital (Díaz, M. E., 2019).

En concordancia con el tercer objetivo específico, se observó un aumento en la cantidad de investigaciones hechas en el país que respaldan la importancia educativa de la ciberdefensa, lo cual es coherente con el tercer objetivo específico, que consiste en clasificar y categorizar fuentes académicas para apoyar la propuesta curricular. La investigación más reciente (Rivera Alturo, L. M., & Hernández García, S. A., 2023) subraya la importancia de instruir a los suboficiales en el uso de herramientas digitales y ciberseguras para potenciar sus habilidades operativas. Para Colombia, es fundamental contar con una legislación específica en ciberdefensa y ciberseguridad (Pacheco, J. A., 2022). Esto debería incorporarse en la capacitación militar a través de la enseñanza sobre los marcos normativos, tanto nacionales como internacionales, que son importantes para el conflicto digital.

La inclusión de la asignatura de guerra cibernética como materia, en términos pedagógicos, podría robustecer el pensamiento crítico, la conciencia tecnológica y la ética profesional de los líderes militares que están por venir. El aprendizaje basado en simulaciones, entornos virtuales y estudios de casos estimularía un aprendizaje situado y significativo, que se ajusta a la cognición situada y al aprendizaje fundamentado en problemas (Brown et al., 1989; Dunleavy et al., 2008). Estos métodos transforman el aula en un espacio de experimentación donde los estudiantes desarrollan habilidades prácticas en situaciones reales de riesgo cibernético. De esta manera, se crea una cultura institucional que prioriza la resiliencia estratégica y la seguridad digital.

Por último, los resultados logrados permiten concluir que es esencial incorporar de manera formal la asignatura de guerra cibernética en el programa educativo militar para fortalecer la defensa del país, impulsar la innovación tecnológica y consolidar una doctrina adecuada para el siglo XXI. Incorporar lo mencionado no se refiere únicamente a renovar el conocimiento, sino que también tiene como meta el desarrollo integral del militar colombiano, que esté preparado en términos técnicos, cognitivos y éticos para enfrentar las nuevas amenazas en el ciberespacio. Esta metodología debe ser complementada con una política institucional de cooperación a nivel internacional, inversión tecnológica e investigación, para asegurar la pertinencia y viabilidad del sistema educativo militar frente a los desafíos presentes en la seguridad mundial.

Referencias Bibliográficas

Acevedo Navas, C., & Fernández Osorio, A. E. (Junio de 2023). *Ejes temáticos estratégicos en seguridad y defensa en Colombia*. Revista Científica General José María Córdova, 21(42), 11–28. Obtenido de https://revistacientificaesmic.com/index.php/esmic/issue/view/39/52

Antonio, J. M. (25 de Enero de 2021). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior*. 53, 198, 169-197. Santiago, Santiago, Chile: Instituto de Estudios Internacionales Universidad de Chile. Obtenido de https://www.scielo.cl/pdf/rei/v53n198/0719-3769-rei-53-198-00169.pdf?utm_source=chatgpt.com

Arciniegas Londoño, L., & Arcila Martínez, L. Y. (09 de Noviembre de 2023). *El rol del Ejército de Liberación Nacional en los dominios de tierra, ciberespacio y cognitivo en el escenario de conflicto armado colombiano*. Revista Perspectivas en Inteligencia, 15(24), 117-138. Obtenido de https://revistascedoc.com/index.php/pei/article/view/666/695

Arquilla, J., & Ronfeldt, D. (24 de Septiembre de 2007). *Cyberwar Is Coming "SE ACERCA LA CIBERGUERRA"*. 141–165. California, California, EE.UU: RAND Corporation. Obtenido de https://www.tandfonline.com/doi/abs/10.1080/01495939308402915

Asamblea Nacional Constituyente. (1991). *Constitución Política de Colombia*. 108. Bogotá D.C., Cundinamarca, Colombia: Asamblea Nacional Constituyente. Obtenido de https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf

Ausubel, D. (1983). *Teoría del aprendizaje significativo*. 1-10. Fascículos de CEIF. Obtenido de https://n9.cl/1qh33

Barrero, J. C. (16 de Abril de 2025). *Política de Educación para la Fuerza Pública 2021-2026: Análisis y comparación con países de la región*. Revista Científica General José María Córdova, 23(50), 510-535. Obtenido de https://revistacientificaesmic.com/index.php/esmic/article/view/1487/1449

Booth, A., Sutton, A., & Papaioannou, D. (19 de Abril de 2016). *Systematic approaches to a successful literature review*. (2nd ed.). Obtenido de https://uk.sagepub.com/sites/default/files/upm-assets/78595_book_item_78595.pdf

Brown, J. S., Collins, A., & Duguid, P. (Enero de 1989). *Cognición situada y la cultura del aprendizaje.* 18(1), 32-42. Educational Researcher. Obtenido de https://journals.sagepub.com/doi/10.3102/0013189X018001032

Colombia, S. F. (2024*). Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CS)*. 1. Bogota D.C., Cundinamarca, Colombia. Obtenido de https://www.superfinanciera.gov.co/publicaciones/10115571/indicadores-de-seguridad-de-la-informacion-y-ciberseguridad-2024/

Camacho, J. D. (2016). *Evolución de la ciberdefensa y la seguridad de la información en Colombia.* 23. Bogotá D.C., Cundinamarca, Colombia: Universidad Militar Nueva Granada. Obtenido de https://repository.umng.edu.co/server/api/core/bitstreams/28a40a02-cd72-403a-8847-7c792876ebbc/content

Centro Cibernético Policial. (2024). *Informe anual de ciberseguridad y defensa nacional. Bogotá D.C.*: Policía Nacional de Colombia. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/observatorio/BALANCE%20ANUAL%20CECIP%202024_1.pdf

Centro de Doctrina del Ejército. (Febrero de 2020). *Doctrina Damasco: Un nuevo pensamiento militar colombiano, referente y guía de transformación para el Ejército Nacional*. Experticia Militar, 9, 84. Obtenido de https://www.cedoe.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/486070/experticia_9_febrero_2020_compressed_2.pdf?utm_source

Congreso de la República de Colombia. (23 de Noviembre de 2001/2018). *Ley 1928 de 2018 "Por medio de la cual se aprueba el 'Convenio sobre la Ciberdelincuencia', adoptado en Budapest el 23 de noviembre de 2001"*. Bogotá D.C., Colombia: Función Pública.

Obtenido de https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_1928_2018.htm

Congreso de la República de Colombia. (05 de Enero de 2009). *Ley 1273 de 2009 Por medio de 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 infor. Bogotá D.C.*, Colombia: Congreso de la República de Colombia. Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (17 de Octubre de 2012). *Ley Estatutaria 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.* Bogotá D.C., Cundinamarca, Colombia: Congreso de la República de Colombia. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (17 de Abril de 2013). *Ley Estatutaria 1621 de 2013 fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia*. Bogotá D.C., Cundinamarca, Colombia: Congreso de la República de Colombia. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Cortez, G. M. (30 de junio de 2024). *Proyecto de formación de oficiales en gerencia tecnológica y diseño de sistemas digitales para la ciberdefensa*. 3, 5, 60-87. Bogotá D.C., Cundinamarca, Colombia: Editorial ESDEG. Obtenido de https://esdegrevistas.edu.co/index.php/rcit/article/view/4861/5276

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiro, J. A. (01 de Abril de 2020). *Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares*. Revista Científica General José María Córdova, 18(30), 357–377. Obtenido de https://revistacientificaesmic.com/index.php/esmic/article/view/588/666

Departamento Nacional de Planeación. (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa (CONPES 3701)*. Bogotá D.C.: Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf

Departamento Nacional de Planeación. (2016). *Política Nacional de Seguridad Digital (CONPES 3854)*. Bogotá D.C.: Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2020). *Política Nacional de Confianza y Seguridad Digital (CONPES 3995)*. Bogotá D.C.: Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Díaz Acevedo, M., & Cremades Guisado, Á. (30 de Diciembre de 2024). *Revisión del estado actual de la ciberseguridad en Colombia*. 19, 38, 180-201. Bogotá D.C., Cundinamarca, Colombia: Editorial ESDEG. Obtenido de https://esdegrevistas.edu.co/index.php/resd/article/view/1999/5308

Díaz, M. E. (2019*). Estrategia militar de ciberdefensa para las fuerzas militares de Colombia de cara a las amenazas cibernéticas que imponen las tecnologías disruptivas al 2022*. 129. Bogotá D.C., Cundinamarca, Colombia: Editorial ESDEG. Obtenido de https://www.esdegrepositorio.edu.co/handle/20.500.14205/4309

Dunleavy, M., Dede, C., & Mitchell , R. (03 de Septiembre de 2008). *Posibilidades y limitaciones de las simulaciones inmersivas participativas de realidad aumentada para la enseñanza y el aprendizaje*. 18, 7-22. J Sci Educ Technol. Obtenido de https://doi.org/10.1007/s10956-008-9119-1

Escuela Superior de Guerra. (18 de Octubre de 2024). *Ejercicio de Simulación en Escenarios de Análisis de Crisis.* Bogotá D.C., Cundinamarca, Colombia: Escuela Superior de Guerra. Obtenido de https://esdegue.edu.co/es/ejercicio-de-simulacion-en-escenarios-de-analisis-de-crisis?utm_source

Escuela Superior de Guerra. (07 de Abril de 2025). esdegue.edu.co. Obtenido de https://esdegue.edu.co/es/diplomado-en-ciberseguridad-y-ciberdefensa?utm_source

Escuela Superior de Guerra. (2025). Escuela Superior de guerra. Maestría en Ciberseguridad y Ciberdefensa, 5. Bogotá D.C., Cundinamarca, Colombia: esdegue. Obtenido de https://esdegue.edu.co/es/maestria-en-ciberseguridad-y-ciberdefensa

Foro Económico Mundial. (2024). *Global Cybersecurity Outlook 2024*. Foro Económico Mundial. Davos - Suiza: World Economic Forum. Obtenido de https://es.weforum.org/publications/global-cybersecurity-outlook-2024/

Fortinet. (2024). *Brecha de Competencias en Ciberseguridad 2024*. (Fortinet, Editor) Obtenido de Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/reports/es_la/2024-cybersecurity-skills-gap-report.pdf

Gamboa, J. A. (30 de Diciembre de 2023). *Competencias digitales del mando militar en el marco DigComp 2.2: caso Escuela Militar de Cadetes "General José María Córdova".* Revista Ciberespacio, Tecnología e Innovación, 2(4), 107-146. Obtenido de https://esdegrevistas.edu.co/index.php/rcit/article/view/4810/5226

Libicki, M. C. (10 de Septiembre de 2009). *Ciberdisuasión y ciberguerra. 240*. California, California, EE.UU: Corporation, RAND. Obtenido de RAND: https://www.rand.org/pubs/monographs/MG877.html

Linares Espinós, E., Hernández, E., Domínguez Escrig, J., Fernández Pello, S., Hevia, V., Mayor, J., . . . Ribal, M. (Octubre de 2018). *Metodología de una revisión sistemática*. 42. Actas Urológicas Españolas - ScienceDirect. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0210480618300615

Lindsay, J., Ming Cheung, T., & Reveron, D. (01 de Abril de 2015). IGCC. (O. U. Press, Ed.) Obtenido de https://ucigcc.org/publication/china-and-cybersecurity-espionage-strategy-and-politics-in-the-digital-domain/

López, A. F., & Velásquez, L. (01 de Diciembre de 2021). *Lineamientos desde el sector defensa para enfrentar campañas de manipulación social hostil que se gestan en Colombia a través del ciberespacio*. Estudios en Seguridad Y defensa, 16(32), 343-378. Obtenido de https://esdegrevistas.edu.co/index.php/resd/article/view/321/423

Mozo Rivera, O., & Ardila Contreras, J. V. (09 de Diciembre de 2022). *El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia*. Revista Científica en Ciencias Sociales e Interdisciplinaria, 14(23), 63-95. Obtenido de https://revistascedoc.com/index.php/pei/article/view/333/729

Nye, J. S. (Mayo de 2010). *Ciberpoder*. 1-19. Massachusetts, EE.UU: Harvard Kennedy School (HKS). Obtenido de https://www.belfercenter.org/publication/cyber-power

O.N.U. (2015). *Objetivos y metas de desarrollo sostenible*. (O. d. Unidas, Editor) Obtenido de https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

Organización de los Estados Americanos (OEA). (2016). *Observatorio de La Ciberseguridad en América Latina y el Caribe*. OEA. Organización de los Estados Americanos (OEA). Obtenido de https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=744&lang=1

Pacheco, J. A. (30 de Junio de 2022). *Importancia de una Ley de ciberseguridad y ciberdefensa para Colombia.* Revista Ciberespacio, Tecnología e Innovación, 1(1), 67-90. Obtenido de https://esdegrevistas.edu.co/index.php/rcit/article/view/4766/5109

Pardo, J. M. (Junio de 2024). *Normatividad para la protección cibernética de la infraestructura crítica en Colombia.* Ciberespacio, Tecnología e Innovación, 3(5), 7–32. Obtenido de https://esdegrevistas.edu.co/index.php/rcit/article/view/4873/5274

Realpe Diaz, M. E., & Cano Martinez, J. J. (09 de Abril de 2020). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional.* Reflexiones y perspectivas en Colombia. 105-112. Bogotá D.C., Cundinamarca, Colombia: Editorial Universidad del Rosario. Obtenido de https://editorial.urosario.edu.co/pub/media/hipertexto/rosario/anexos/proyecto-cibsi/10_S7_ok.pdf

Rid, T. (05 de Octubre de 2011). *La guerra cibernética no tendrá lugar.* Revista de Estudios Estratégicos, 35(1), 5-32. Obtenido de

https://www.tandfonline.com/doi/full/10.1080/01402390.2011.608939?scroll=top&needAccess=true

Ringas, E. E., Kerttunen, M., & Spirito, C. (30 de Septiembre de 2014). *La ciberseguridad como campo de estudio y educación militar*. Prensa de la Universidad de Defensa Nacional. Obtenido de https://ndupress.ndu.edu/Joint-Force-Quarterly/Joint-Force-Quarterly-75/Article/577562/cyber-security-as-a-field-of-military-education-and-study/

Rivera Alturo, L. M., & Hernández García, S. A. (18 de Diciembre de 2023). *La ciberseguridad un enfoque de aprendizaje, desde el rol del suboficial del Ejército Nacional de Colombia*. Revista de investigación Miradas, 18(2), 191-204. Obtenido de https://revistas.utp.edu.co/index.php/miradas/article/view/25519/17214

Rodríguez, A. G. (04 de Diciembre de 2015). *Cibernética en la guerra contemporánea: definición de nuevos escenarios estratégicos y operacionales.* Revista Escuela Superior de Guerra, 10(20), 117-131. Obtenido de https://esdegrevistas.edu.co/index.php/resd/article/view/41/24

Rodríguez, P. A. (30 de Junio de 2025). *Operaciones cibernéticas en el nivel operacional de la guerra: lecciones del conflicto entre Rusia y Ucrania.* Revista Ciberespacio, Tecnología e Innovación, 4(7), 15-40. Obtenido de https://esdegrevistas.edu.co/index.php/rcit/article/view/4942/5417

Suarez, J. S. (09 de Noviembre de 2023). *Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital*. Perspectivas en Inteligencia, 15(24), 333–359. Obtenido de https://doi.org/10.47961/2145194X.628

Valeriano, B., & Maness, R. (18 de Noviembre de 2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* Revista de Tecnología de la Información y Política, 399-401. Obtenido de https://www.researchgate.net/publication/284196184_Book_Review_Cyber_War_Versus_Cyber_Realities_Brandon_Valeriano_and_Ryan_C_Maness

Apéndices

Apéndices A

Ficha RAE (Resumen Analítico Especializado) Para el Análisis de la Literatura Consultada.

	RAE (Resumen Analítico Especializado)
Tipo de Documento:	Monografía
Acceso al Documento:	Abierto
Título del Documento:	Revisión sistemática de los fundamentos doctrinales, pedagógicos y tecnológicos para la inclusión de la guerra cibernética como asignatura en la doctrina militar de Colombia.
Autor(es):	Derwin Martínez Rodríguez
Director(a) / Asesor(a):	Jhon Manuel Soto
Año de la Publicación:	Villavicencio – Meta 2025
Palabras Claves:	Asignatura de guerra cibernética, Doctrina militar, Ciberdefensa, PRISMA 2020, Revisión Sistemática.
Descripción del Contenido: (Resumen Analítico)	La finalidad de este trabajo de grado es analizar la importancia y los fundamentos para incluir la guerra cibernética como una asignatura, materia o tema central en el plan de estudio de la doctrina militar colombiana, en concordancia con estrategias pedagógicas que verifiquen competencias doctrinales y digitales relacionadas con guerra cibernética. Para ello se realiza una revisión sistemática, empleando la metodología PRISMA 2020, para establecer una propuesta de currículo que respalde la inclusión de la materia de guerra cibernética en la doctrina militar colombiana. Esta revisión abarca las evidencias publicadas entre los años 2020 y 2025 sobre la guerra cibernética y su impacto en la doctrina militar. En este orden de ideas, "Ciberdefensa y Guerra Cibernética" se convierte en un componente de suma importancia para el currículo militar, cuyo objetivo es que el personal sea capacitado de manera integral en los niveles técnico, profesional y especializado. La propuesta curricular incluye el uso de herramientas tecnológicas modernas, tales como simulaciones, plataformas digitales que generan una sensación de presencia y realismo, laboratorios virtuales y ejercicios prácticos de defensa y

	ciberataque. Estos instrumentos ayudan a que los estudiantes interactúen con situaciones digitales hipotéticas o reales de conflicto. Por lo tanto, la asignatura contribuirá significativamente a fortalecer la doctrina militar del país, promoviendo una cultura institucional de renovación tecnológica y de autoridad. Asimismo, la actualización permanente de los integrantes del Ejército Nacional se fomentará como parte de una estrategia integral de ciberdefensa que enfrenta los desafíos que plantean las tecnologías disruptivas.
Objetivos:	**Objetivo General** Realizar una revisión sistemática de la literatura sobre guerra cibernética en currículos y bases doctrinales, para formular una propuesta curricular que fundamente la inclusión de la asignatura de guerra cibernética en la doctrina militar colombiana. **Objetivos Específicos** Identificar la consecuencia de la guerra cibernética en la doctrina militar de Colombia y cómo se refleja en el desarrollo de tácticas defensivas innovadoras y contextos operativos contemporáneos. Establecer las nociones doctrinales, pedagógicas y tecnológicas que respalden la inclusión de la guerra cibernética como materia en el entrenamiento militar, de acuerdo con las políticas educativas y de defensa nacional. Clasificar y sistematizar las fuentes doctrinales, académicas y científicas pertinentes para establecer un marco de referencia que apoye la propuesta curricular en el ámbito de ciberdefensa.
Área del Conocimiento o Disciplina:	Escuela de Ciencias Básicas Tecnología e Ingeniería - Ingeniería de Sistemas

Nota. Documento académico de acceso abierto que presenta una revisión sistemática bajo metodología PRISMA 2020 y propone la inclusión curricular de la guerra cibernética en la doctrina militar colombiana. Adaptada de *"Revisión sistemática de los fundamentos doctrinales, pedagógicos y tecnológicos para la inclusión de la guerra cibernética como asignatura en la doctrina militar de Colombia"*, (2025), Elaboración propia (Martínez R.D., 2025).