Capítulo

Ciberarmas y disuasión en Colombia: Un marco estratégico para la defensa nacional*

Juan Carlos García Ruíz
Estudiante del Curso de información Militar y Especialización en Seguridad y Defensa

William Yamit Castro Mendoza
Estudiante del Curso de información Militar y Especialización en Seguridad y Defensa

Alejandro Jose Maestre Rodriguez
Estudiante del Curso de información Militar y Especialización en Seguridad y Defensa

Resumen: El presente artículo explora el desarrollo de ciberarmas como una ventaja estratégica para la defensa y seguridad nacional, con un enfoque, que este desarrollo y el fortalecimiento de las capacidades cibernéticas generen una disuasión creíble para Colombia ante amenazas de origen interno y externo. A través de un diseño de investigación mixto y exploratorio, se analiza la evolución doctrinal y operativa de potencias cibernéticas como Estados Unidos, Rusia, China e Israel, basándose en una revisión sistemática de literatura académica, documentos de política pública, empresas del sector tecnológico. Se argumenta que las ciberarmas, por su naturaleza asimétrica y de bajo costo, ofrecen a países con capacidades militares limitadas una herramienta eficaz para proyectar poder y disuadir a adversarios. Los estudios de caso revelan lecciones cruciales sobre la integración civil-militar, la inversión en talento humano y la importancia de la disuasión por negación. El artículo concluye que, para capitalizar estas ventajas, Colombia debe articular una doctrina de ciberdefensa alineada con marco normativo como la ley de inteligencia, el decreto 338 del 2022, la estrategia de ciberseguridad y los CONPES, debido a la falta de leyes que fortalezcan y regulen esta capacidad, priorizando un modelo de gobernanza que equilibre la necesidad de secreto operativo con el control democrático, mientras se fomenta la innovación y la cooperación estratégica. Este trabajo cierra una brecha crítica en la literatura al proponer un marco conceptual y recomendaciones pragmáticas para la política de ciberdefensa de

* Capítulo de libro resultado del proyecto de investigación "mencionar proyecto" del grupo de investigación "mencionar grupo" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en XX por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias) y registrado con el código COLXXXXXXX. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Colombia, un país que navega entre la necesidad de seguridad interna y los desafíos de un entorno geopolítico global cada vez más digitalizado.

Palabras clave: Ciberarmas, Ciberseguridad, Ciberdefensa, Disuasión, Colombia, Estrategia Nacional, marco jurídico

Juan Carlos García Ruíz
Ingeniero de sistemas con énfasis en Telecomunicaciones, Universidad Cooperativa de Colombia, Especialista en Seguridad de la información, Universidad Piloto de Colombia, Magister en Ciberdefensa y Ciberseguridad, Escuela Superior de Guerra, Colombia. Estudiante del Curso de información Militar y Especialización en Seguridad y Defensa Nacional, Escuela Superior de Guerra, Colombia. https://orcid.org/0000-0002-7338-0710- Contacto: juan.garcia@esdeg.edu.co

William Yamit Castro Mendoza
Especialista en Medicina Critica y Cuidados Intensivos, Universidad De Cartagena, Especialista en Cirugía General, Universidad Militar Nueva Granada, Medicina General, Universidad del Sinú Seccional Cartagena, Estudiante del Curso de información Militar y Especialización en Seguridad y Defensa Nacional, Escuela Superior de Guerra- ORCID ID: 0000-0002-6119-5513 Contacto: william.castro@esdeg.edu.co

Alejandro Jose Maestre Rodriguez
Ingeniero Electricista, Universidad de Pamplona, Colombia. Estudiante del Curso de información Militar y Especialización en Seguridad y Defensa Nacional, Escuela Superior de Guerra, Colombia, https://orcid.org/0009-0008-3674-9722- Contacto: alejandro.maestre@esdeg.edu.co

[T1] Introducción

La progresiva digitalización de las sociedades contemporáneas y la interconexión global han reconfigurado radicalmente el panorama de la seguridad y la defensa. En este nuevo escenario, el ciberespacio ha emergido no solo como un facilitador de la vida moderna, sino también como un nuevo dominio de confrontación y conflicto. La ciberguerra, definida como el uso de ataques digitales por parte de un Estado para dañar, degradar, interrumpir, sabotear los sistemas informáticos más esenciales de otra nación, se ha consolidado como una realidad tangible que complementa, y en ocasiones supera, las formas tradicionales de enfrentamiento (LISA Institute, s.f.-b). Las ciberarmas, herramientas diseñadas para explotar vulnerabilidades en sistemas y redes con fines hostiles, son los instrumentos de este nuevo tipo de guerra, capaces de generar un espectro de efectos que van desde la interrupción de servicios básicos y el espionaje a gran escala, hasta el sabotaje de infraestructuras críticas y la desestabilización de naciones enteras (Avast, s.f.; Duque-Grajales et al., 2023). La creciente dependencia de infraestructuras digitales interconectadas magnifica la amenaza y el impacto potencial de estas armas, convirtiéndolas en un elemento central de la seguridad nacional y las relaciones internacionales (Duque-Grajales et al., 2023).

El presente articulo aborda la pregunta de investigación: ¿En qué medida el desarrollo y despliegue de ciberarmas puede generar ventajas estratégicas sostenibles para las Fuerzas Militares de Colombia y aportar en la política de defensa y seguridad nacional? La relevancia de esta cuestión para Colombia es multifacética. En un contexto de recursos limitados y la necesidad de desarrollar capacidades asimétricas, las ciberarmas ofrecen la promesa de una ventaja estratégica a un costo potencialmente menor que el armamento cinético tradicional, con un poder disuasorio creíble frente a una variedad de amenazas, tanto externas como internas. La capacidad de proyectar poder en el ciberespacio, de disuadir agresiones y de responder eficazmente a los ataques se ha convertido en un imperativo para los Estados que buscan salvaguardar su soberanía y sus intereses vitales en el siglo XXI.

El objetivo general de este estudio es describir la medida en que el desarrollo y despliegue de ciberarmas puede generar ventajas estratégicas sostenibles para las Fuerzas Militares de Colombia y, a partir de este análisis, diseñar una estrategia integral que permita capitalizar dichas ventajas en el marco de su política de defensa y seguridad nacional. Para alcanzar este fin, se han establecido los siguientes objetivos específicos:

- Caracterizar las ciberarmas, sus ventajas, desventajas, impacto y poder, tomando como referencia a Estados Unidos, Rusia, China y Corea del Norte (incluidas sus Amenazas Persistentes Avanzadas o APTs asociadas), con el fin de establecer tipologías y niveles de sofisticación relevantes para el contexto colombiano.

- Analizar casos representativos del empleo de ciberarmas por parte de esos mismos Estados, con el fin de extraer lecciones estratégicas, tecnológicas y doctrinales aplicables al diseño y despliegue de capacidades en Colombia.

- Diseñar una estrategia integral para el desarrollo y uso de ciberarmas para las Fuerzas Militares de Colombia, que establezca líneas de acción en investigación y desarrollo (I+D), talento humano, cooperación internacional y gobernanza, junto con indicadores de sostenibilidad y efectividad.

Este informe se estructura en cuatro capítulos principales. El Capítulo 1 establece los fundamentos conceptuales de las ciberarmas y la ciberguerra. El Capítulo 2 analiza las capacidades y doctrinas de ciberarmas de actores estatales relevantes. El Capítulo 3 examina estudios de caso emblemáticos para extraer lecciones aplicables. Finalmente, el Capítulo 4 propone una estrategia integral para el desarrollo y empleo de ciberarmas por parte de las Fuerzas Militares de Colombia. Las conclusiones sintetizarán los hallazgos y ofrecerán recomendaciones estratégicas.

2. Marco Teórico y Revisión de la Literatura

2.1. Ciberespacio y Ciberarmas: Fundamentos Conceptuales y Potencial Estratégico

El ciberespacio, un "dominio global virtual", ha evolucionado de una simple infraestructura de apoyo a las comunicaciones a un escenario estratégico de confrontación (Argumosa, 2022). A diferencia de los dominios físicos, este es un entorno artificial, "creado por el hombre", que se compone de varias capas: una capa de red física (hardware, cables), una capa de red lógica (software, protocolos) y una capa de ciber-persona (identidades online, información) (Medina Ochoa, 2019). Esta naturaleza multicapa implica que las operaciones cibernéticas pueden dirigirse a diferentes aspectos de un sistema, desde el hardware hasta la percepción humana. Esta complejidad no solo dificulta la defensa y la atribución, sino que también subraya la naturaleza de doble uso de muchas herramientas, que pueden servir para fines civiles o militares.

La ciberguerra, entendida como el uso de ataques digitales respaldados por un Estado para dañar los sistemas de otra nación, se ha consolidado como una realidad. Las ciberarmas son los instrumentos de este nuevo tipo de guerra, diseñadas para explotar vulnerabilidades y generar efectos que van desde el espionaje hasta el sabotaje de infraestructuras críticas (LISA Institute, s.f.-b; Avast, s.f.). A diferencia del armamento cinético, las ciberarmas permiten

una intervención asimétrica y de bajo costo, lo que las hace particularmente atractivas para estados con recursos limitados.

Se clasifican las ciberarmas según su propósito:

- Ofensivas: Proyectan poder para dañar o destruir sistemas.
- Defensivas: Protegen los sistemas propios y mitigan ataques.
- Doble Uso: Capacidades que pueden ser empleadas tanto con fines ofensivos como defensivos.

Según su efecto, las operaciones pueden ser de espionaje (robar información), sabotaje/ataque (interrumpir funcionalidad), propaganda/desinformación (influir en la opinión pública) o disrupción económica (causar pérdidas financieras). La sofisticación de estas herramientas varía enormemente. Las Amenazas Persistentes Avanzadas (APTs) son campañas de ciberataque de alta complejidad, orquestadas por estados o grupos patrocinados, que buscan establecer una presencia continua y no detectada en una red para el espionaje a largo plazo o la preparación de futuros ataques (Kaspersky, 2025). Ejemplos notables incluyen Stuxnet, un gusano informático que causó daño físico a las centrifugadoras nucleares de Irán, y NotPetya, un wiper disfrazado de ransomware que causó pérdidas globales (Greenberg, 2018).

A pesar de sus ventajas, las ciberarmas presentan desventajas significativas. Su vida útil es corta, ya que las vulnerabilidades que explotan pueden ser parchadas (EBSCO, s.f.). Además, existe un alto riesgo de proliferación no intencionada, como se vio con Stuxnet, cuyo código fue adaptado y reutilizado por otros actores (Bachkatov, 2010; Stoddart, 2022). La dificultad de atribución y el vacío de gobernanza internacional complican la aplicación de la ley y aumentan el riesgo de escalada (Reinhold & Reuter, 2023).

2.2. Ventajas, Desventajas e Impacto Estratégico de las Ciberarmas

El desarrollo y empleo de ciberarmas conllevan un conjunto complejo de ventajas estratégicas, desventajas inherentes y un impacto profundo en la seguridad y las relaciones internacionales. Las ciberarmas ofrecen múltiples ventajas que las hacen atractivas para los actores estatales. Una de las más citadas es el bajo costo relativo y la capacidad de generar asimetría (Duque-Grajales et al., 2023; Goines, 2019). Permiten a los Estados, especialmente aquellos con presupuestos de defensa más limitados, proyectar poder e influir en adversarios sin incurrir en los enormes gastos asociados con las operaciones militares convencionales. La capacidad de "nivelar el campo de juego" es particularmente relevante en un mundo donde

las disparidades en poder militar convencional son significativas (Duque-Grajales et al., 2023).

El potencial disuasorio es otra ventaja clave. Las ciberarmas pueden ser empleadas como una forma de coerción, enviando mensajes claros a otros actores internacionales y amenazando con consecuencias significativas si no se cumplen ciertas condiciones o si se cruzan determinadas líneas rojas (Duque-Grajales et al., 2023; Goines, 2019). La mera posesión de capacidades ciberofensivas creíbles puede disuadir a un adversario de emprender acciones hostiles.

La naturaleza de las operaciones cibernéticas permite un alto grado de encubrimiento y dificulta la atribución (Duque-Grajales et al., 2023; EBSCO, s.f.). Los ataques pueden lanzarse desde cualquier parte del mundo, a través de múltiples intermediarios y utilizando técnicas de ofuscación, lo que complica la identificación del origen y permite a los atacantes mantener una "negación plausible". Esta característica reduce el riesgo de represalias inmediatas y directas.

Además, las ciberarmas pueden ofrecer precisión y selectividad, permitiendo afectar objetivos clave (sistemas de mando y control, infraestructuras específicas, bases de datos) sin necesidad de una fuerza militar convencional masiva y con un menor riesgo de daño colateral indiscriminado, si se diseñan y emplean cuidadosamente (Duque-Grajales et al., 2023). Finalmente, no se debe subestimar el impacto psicológico y en la opinión pública que pueden generar los ciberataques, erosionando la confianza en el gobierno, sembrando el caos o manipulando la percepción de la realidad (LISA Institute, s.f.-b; Avast, s.f.).

No obstante, las ciberarmas también presentan importantes desventajas que limitan su utilidad estratégica. Una de ellas es su corta vida útil y rápida obsolescencia (EBSCO, s.f.; Goines, 2019). Las vulnerabilidades que explotan pueden ser descubiertas y parchadas por los fabricantes de software o los administradores de sistemas, volviendo ineficaces los exploits desarrollados. Esto exige una inversión continua en investigación y desarrollo para mantener un arsenal relevante.

Las consecuencias imprevisibles y el riesgo de daño colateral son preocupaciones mayores (EBSCO, s.f.; Secureframe, 2024). El código malicioso, una vez liberado, puede propagarse sin control y afectar a sistemas y países no previstos, como demostraron los incidentes de WannaCry y NotPetya, que causaron miles de millones en pérdidas a nivel global (Greenberg, 2018; Kaspersky, 2017; Cloudflare, 2025). Este "efecto boomerang" puede tener repercusiones diplomáticas y económicas graves.

Relacionado con lo anterior, existe un alto riesgo de proliferación y reutilización (LISA Institute, s.f.-b; Secureframe, 2024). Una vez que una ciberarma es desplegada y detectada, puede ser analizada, copiada, modificada y reutilizada por otros actores, incluyendo adversarios o incluso grupos criminales. El código de Stuxnet, por ejemplo, sirvió de base o inspiración para otras herramientas maliciosas (Trellix, 2025).

El llamado "cyber weapons paradox" o "paradoja de las ciberarmas" (Goines, 2019) plantea un dilema estratégico: el uso abierto y visible de una ciberarma con fines disuasorios (para que el adversario conozca la capacidad y la voluntad de usarla) puede comprometer su efectividad para operaciones encubiertas futuras, ya que revela sus características y permite el desarrollo de contramedidas.

Finalmente, los desafíos legales y éticos son considerables. La ausencia de un marco normativo internacional claro y universalmente aceptado para la ciberguerra, la dificultad de aplicar el Derecho Internacional Humanitario (DIH) a los ciberconflictos, y las cuestiones sobre proporcionalidad y distinción, generan un entorno de incertidumbre y riesgo de escalada (LISA Institute, s.f.-b; Duque-Grajales et al., 2023).

Tabla 1: Ventajas y Desventajas de las Ciberarmas vs. Armamento Cinético

Característica	**Ciberarmas**	**Armamento Cinético**
Costo de desarrollo	Bajo	Muy Alto
Atribución	Difícil / Anónima	Directa
Escalada	Impredecible / 'Zona Gris'	Alta / Predictible
Proliferación	Alta (copia y modificación)	Baja (requiere manufactura)
Efectos	Reversibles y no cinéticos, hasta cinéticos	Principalmente cinéticos e irreversibles

Desarrollo propio utilizando promt de inteligencia artificial - Gemini

2.3. El Framework MITRE ATT&CK: Un Enfoque para la Caracterización de Amenazas

Para una caracterización rigurosa de las ciberarmas y las amenazas, es indispensable utilizar un marco de referencia estandarizado que vaya más allá de las definiciones teóricas y se centre en el comportamiento observable de los adversarios. El MITRE ATT&CK™ (Adversarial Tactics, Techniques, and Common Knowledge) es un framework globalmente accesible que se ha convertido en el estándar de la industria y el gobierno para describir y categorizar las tácticas y técnicas de ciberataque basadas en observaciones del mundo real (CISA, 2021; MITRE, 2019b).

El ATT&CK organiza el comportamiento de los adversarios en tres niveles jerárquicos:

1. Tácticas: Representan los objetivos técnicos de un adversario, es decir, el "porqué" de una acción. El framework de ATT&CK para empresas define 14 tácticas, como "Acceso Inicial" (Initial Access), "Ejecución" (Execution), "Persistencia" (Persistence), "Movimiento Lateral" (Lateral Movement) y "Exfiltración" (Exfiltration) (MITRE, 2024b). Estas tácticas visualizan las fases del ciclo de vida de un ataque cibernético.

2. Técnicas: Describen el "cómo" un adversario logra un objetivo táctico. Por ejemplo, para lograr la táctica de "Persistencia", un adversario puede utilizar la técnica de "Tarea Programada" (Scheduled Task/Job) para asegurar que su código se ejecute en el futuro (MITRE, 2024b). El ATT&CK documenta más de 100 técnicas observadas en el mundo real.

3. Procedimientos: Son implementaciones específicas y concretas de una técnica o sub-técnica por parte de un grupo de amenazas. Por ejemplo, el grupo APT28 (Fancy Bear) utiliza una técnica de spear-phishing (sub-técnica de la táctica de acceso inicial) de una manera particular.

La matriz de ATT&CK proporciona un "mapa de calor" visual para entender qué técnicas son más comunes o de mayor prioridad para una organización (MITRE, 2019b; CISA, 2021). Este framework es una herramienta poderosa para:

- Inteligencia de Amenazas: Mapear los comportamientos de un adversario conocido (como APTs rusas o chinas) a las técnicas del ATT&CK permite a los defensores entender cómo los atacantes operan y priorizar las defensas.

- Detección y Análisis: Proporciona a los analistas de seguridad los datos y las capacidades de búsqueda que necesitan para identificar comportamientos maliciosos en sus sistemas (MITRE, 2019c).

- Emulación de Adversarios: Permite a los equipos de "red team" (equipos de ataque simulado) replicar las tácticas de un adversario real en un entorno controlado para validar las defensas (MITRE, 2019a).

- Evaluación y Ingeniería de la Defensa: Ayuda a las organizaciones a medir su cobertura defensiva, identificar brechas de seguridad de alta prioridad y guiar las mejoras en la arquitectura de seguridad (MITRE, 2019d).

2.4. Enfoques teóricos y conceptualización de la ciberdefensa estatal

El estudio de la ciberdefensa estatal puede abordarse desde múltiples enfoques teóricos que ayudan a entender cómo los Estados proyectan su poder en el ciberespacio, sus motivaciones y las estrategias que adoptan. Desde una perspectiva realista, la ciberdefensa se concibe como una extensión del poder estatal en un entorno de anarquía, donde la capacidad de respuesta rápida y la disuasión son cruciales para garantizar la supervivencia del Estado (Valeriano & Maness, 2014). El realismo explica la lógica detrás de la carrera de armamentos cibernéticos, donde cada Estado busca maximizar su poder relativo para disuadir a los demás. En este sentido, la adquisición de una capacidad de ciberarmas se ve como una necesidad para la "autoayuda" en un sistema sin una autoridad central. Desde el liberalismo, se enfatiza la importancia de las instituciones internacionales y la cooperación transfronteriza para establecer normas de comportamiento y reducir la incertidumbre inherente al ciberespacio. Los liberales argumentarían que la proliferación de ciberataques solo puede ser gestionada a través de acuerdos multilaterales y la promoción de la confianza mutua. Finalmente, el constructivismo, por su parte, ayuda a entender cómo las identidades y percepciones mutuas entre estados moldean sus intereses y, por lo tanto, sus estrategias en el ciberespacio (Valeriano & Maness, 2014). Los actos de ciberdisuasión no son solo una demostración de poder, sino también una señalización que busca construir una reputación de capacidad y voluntad, lo que es esencial para la disuasión creíble. La percepción de un ataque y la respuesta que un Estado elija dar, o no dar, moldeará su identidad como actor en el ciberespacio y afectará la percepción de su poder por parte de otros Estados.

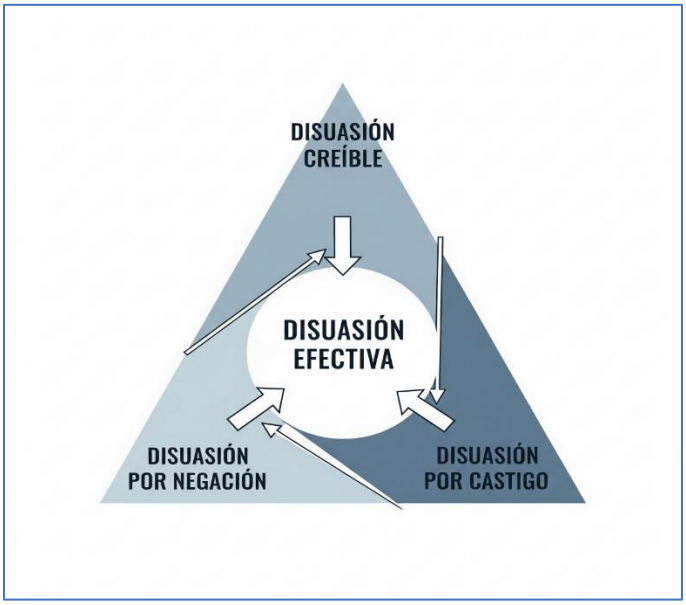


Ilustración 1 El Triángulo de la Disuasión Cibernética

3. Metodología

Este estudio adopta un diseño de investigación mixto secuencial y exploratorio, que combina la revisión sistemática de la literatura con un análisis comparativo de estudios de caso. Este enfoque permite, en una primera fase, la construcción de un marco teórico sólido a partir de la bibliografía académica existente. En una segunda fase, se aplican las lecciones extraídas de casos documentados en literatura académica indexada para responder a la pregunta de investigación y proponer un marco estratégico para Colombia.

3.1. Revisión Sistemática de la Literatura

Para la primera fase, se llevará a cabo una revisión sistemática de la literatura académica siguiendo los principios de la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). El objetivo es identificar, seleccionar y analizar las publicaciones más relevantes en el campo de las ciberarmas, la disuasión cibernética y la seguridad nacional.

- Bases de Datos y Periodo: La búsqueda se realizará en bases de datos indexadas de alto impacto como Scopus, Web of Science (WoS) y Google Scholar, cubriendo el período de 2018 a 2025 para asegurar la actualidad de la información.

- Criterios de Búsqueda: Se utilizarán palabras clave como "cyberweapons", "cyber deterrence", "cyber warfare", "national security strategy", "disuasión cibernética" y "guerra cibernética".

- Criterios de Selección: La selección de artículos se basará en su clasificación en cuartiles Q1 y Q2 para garantizar el rigor y la calidad de las fuentes.

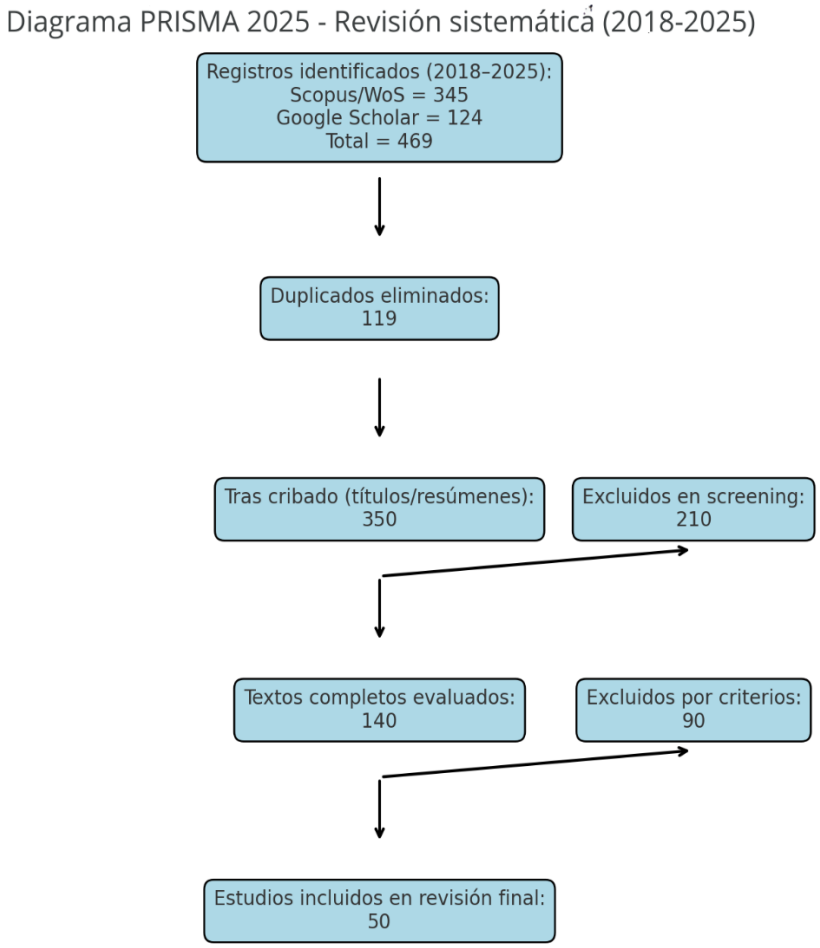


Ilustración 2 PRISMA

3.2. Análisis Comparativo de Estudios de Caso

La segunda fase de la metodología se centra en el análisis cualitativo de estudios de caso. Esta técnica se empleará para profundizar en las estrategias, doctrinas y resultados del desarrollo y despliegue de ciberarmas en países clave. La selección de casos se justifica

por la diversidad de sus aproximaciones estratégicas y su relevancia como potencias cibernéticas.

- Casos de Estudio:
  - Estados Unidos: Se analizará su doctrina de "defensa hacia adelante" y el rol del U.S. Cyber Command.
  - Rusia: Se examinará su uso de ciberarmas en el marco de la guerra híbrida, con especial atención a las operaciones contra Ucrania.
  - China: Se estudiará su enfoque en la superioridad tecnológica y la combinación de ciberataques, inteligencia artificial y operaciones psicológicas.
  - Israel: Se revisará su modelo de innovación civil-militar y el uso de ciberarmas para la disuasión asimétrica.
- Variables de Análisis: Para cada caso, se analizarán las siguientes variables:

1. Tipos de ciberarmas empleadas: (p. ej., malware de sabotaje, herramientas de espionaje).
2. Objetivos estratégicos: (p. ej., disuasión, espionaje, desestabilización).
3. Marco doctrinal y legal: (p. ej., si existen políticas explícitas sobre el uso de ciberarmas).
4. Resultados y lecciones aprendidas: (éxitos y fracasos en la consecución de objetivos).

3.3. Síntesis y Propuesta Estratégica

Finalmente, los hallazgos de la revisión sistemática y el análisis comparativo de casos se sintetizarán para identificar los elementos clave de una estrategia de ciberarmas. Estos elementos servirán de base para proponer un marco estratégico para las Fuerzas Militares de Colombia, que aborde el desarrollo de capacidades, la gobernanza, la cooperación internacional y el fortalecimiento de la disuasión creíble, en línea con los objetivos de esta investigación.

4. Resultados y Análisis de los Casos de Estudio

El análisis comparativo de las estrategias cibernéticas de potencias globales revela distintas aproximaciones al uso de ciberarmas para la disuasión y la proyección de poder. A

continuación, se presentan los hallazgos clave de cada caso de estudio, analizados según las variables establecidas en la metodología.

4.1. Estados Unidos: Doctrina de "Defensa Hacia Adelante" y Dominio Tecnológico

La estrategia de Estados Unidos, articulada por el U.S. Cyber Command, se basa en la doctrina de "defensa hacia adelante" (AFDP 3-12, 2023; Stoddart, 2017). Esta aproximación implica una postura proactiva, operando en redes extranjeras para neutralizar amenazas antes de que alcancen las fronteras nacionales (Parker, 2014). La Fuerza Aérea de EE. UU. considera el ciberespacio un "dominio operacional" donde se realizan ofensivas invisibles e inaudibles, pero tan reales como los ataques convencionales (Parker, 2014).

- Tipos de ciberarmas: La doctrina de la Fuerza Aérea de EE.UU. distingue entre Operaciones Cibernéticas Ofensivas (OCO), que buscan proyectar poder en y a través del ciberespacio, y Operaciones Cibernéticas Defensivas (DCO), para preservar capacidades propias (AFDP 3-12, 2023). El Teniente Coronel Kevin L. Parker (2014) destaca que el ciberespacio es un dominio que favorece la ofensiva debido a su alcance global, la velocidad sin paralelo de sus acciones y la dificultad de atribución. Esta anonimidad permite una "libertad de acción con atribución limitada", lo que es una ventaja táctica significativa (Parker, 2014). El documento "El ciberespacio como zona de control geopolítico..." señala que EE. UU. ha utilizado su control inicial del internet para estrategias de ciberespionaje amplias e innovadoras, incluso contra aliados, lo que ha generado tensión y desconfianza (Rivas, 2021).

- Objetivos estratégicos: El principal objetivo es la disuasión por negación, buscando hacer que los ataques a sus redes sean inútiles (Parker, 2014). Sin embargo, su enfoque ofensivo también sirve como una forma de disuasión por castigo, señalando la capacidad y la voluntad de infligir daño (Parker, 2014). El objetivo es lograr "superioridad cibernética", un grado de dominio que permita la conducción segura de operaciones sin interferencia prohibitiva (AFDP 3-12, 2023).

- Lecciones para Colombia: La doctrina estadounidense subraya la importancia de una integración civil-militar, y la necesidad de talento especializado a gran escala (AFDP 3-12, 2023; Stoddart, 2017). El documento de Parker también introduce la noción de utilizar el "poder blando" del Departamento de Defensa para influir en el sector privado y los aliados a fin de fortalecer las defensas exteriores de manera indirecta (Parker, 2014).

Imagen 1: [Imagen del logo del U.S. Cyber Command]

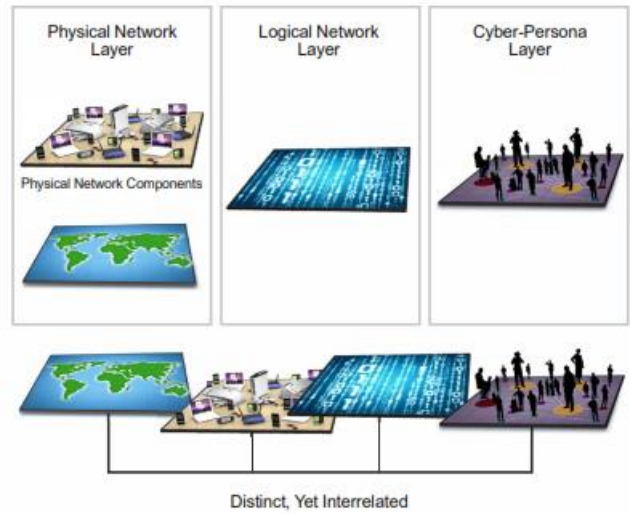


Imagen 1: [Infografía de las tres capas del ciberespacio (física, lógica, de ciber-persona)]
Ilustración 3 tres capas JP3_12 Cyberoperations USA

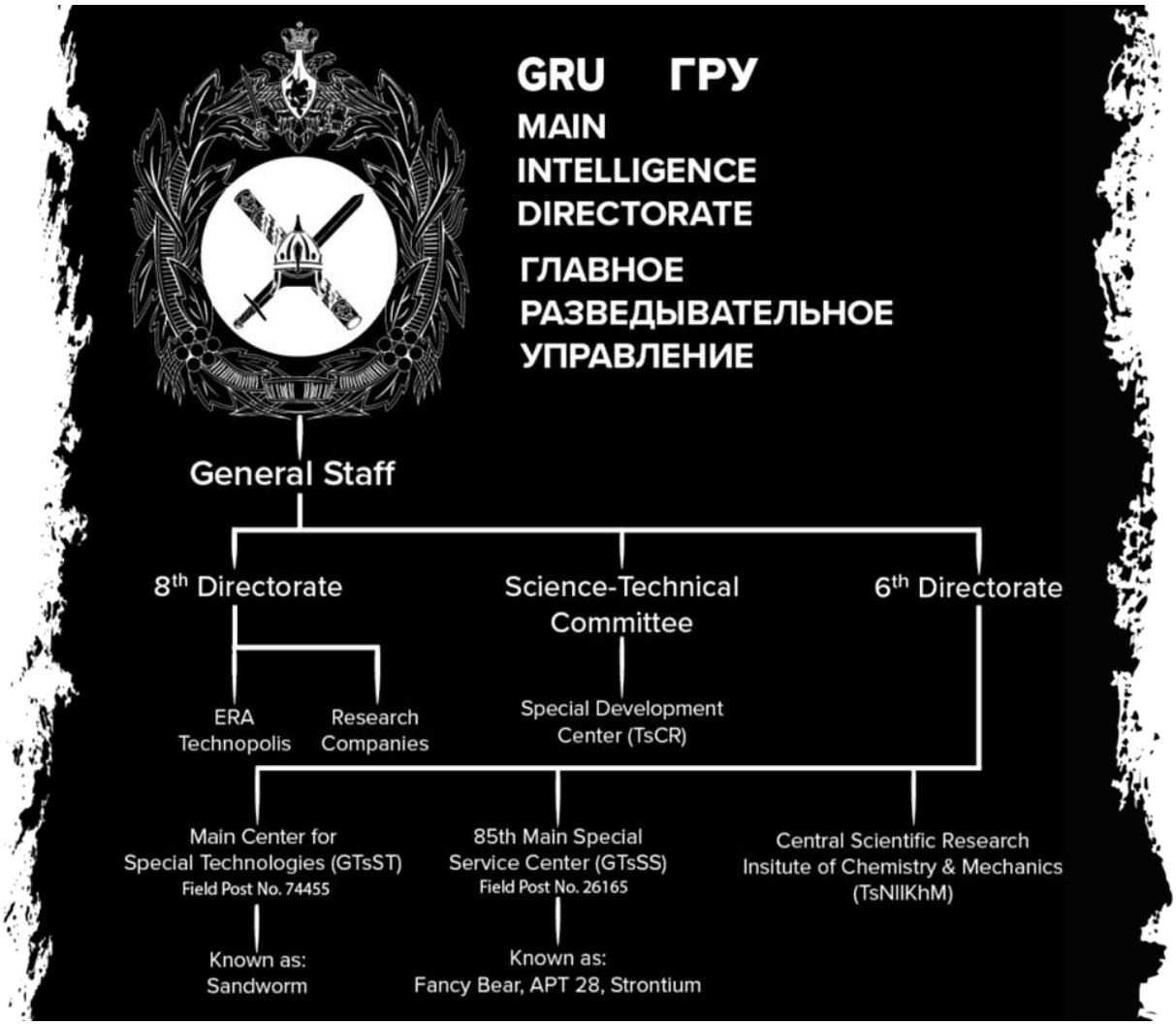
4.2. Rusia: Ciberarmas en el Marco de la Guerra Híbrida

Rusia utiliza las ciberarmas como un componente integral de su estrategia de guerra híbrida, que busca desestabilizar adversarios sin provocar una respuesta militar convencional. El conflicto con Ucrania es el caso más representativo de esta estrategia (IISS, 2024). Las relaciones de Rusia con la OTAN han sido tensas desde la caída de la Unión Soviética, con la expansión de la alianza vista como una "grave amenaza" para la seguridad rusa, lo que ha impulsado un enfoque de defensa nacional más asertivo (Anuario Internacional CIDOB, 2010).

- Tipos de ciberarmas: Se emplean herramientas de ciberespionaje y malware de sabotaje (como NotPetya y las operaciones contra la infraestructura eléctrica ucraniana), combinados con campañas masivas de desinformación y guerra psicológica (Khoirunnisa et al., 2025). Un acuerdo reciente con Irán también muestra la cooperación en ciberseguridad y regulación de internet, lo que refleja un intento de contrarrestar el dominio de las potencias occidentales en el ciberespacio (Stroppa, 2022). Además, el documento "El ciberespacio como zona de control geopolítico..." menciona que Rusia supuestamente utilizó ciberataques para manipular las elecciones de Estados Unidos en 2016, lo que demuestra el uso de ciberarmas con fines de "guerra cognitiva" (Rivas, 2021).

Objetivos estratégicos: Los objetivos son la disrupción sistémica de las capacidades del adversario y la manipulación de la opinión pública (Khoirunnisa et al., 2025). La disuasión rusa opera a través de la ambigüedad y la negación plausible, lo que dificulta la atribución y la respuesta.

- Lecciones para Colombia: Este caso destaca la vulnerabilidad de las infraestructuras críticas ante ataques que combinan el sabotaje con la manipulación informativa (Khoirunnisa et al., 2025). También muestra la importancia de las alianzas estratégicas para contrarrestar la hegemonía de las superpotencias.



https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/

4.3. China: Superioridad Tecnológica e Integración Civil-Militar

La estrategia de ciberseguridad y ciberguerra de China se basa en el objetivo a largo plazo de lograr la superioridad tecnológica. Su enfoque combina el desarrollo de capacidades ofensivas y defensivas bajo un marco doctrinal unificado, con una fuerte integración entre el sector militar, las empresas de tecnología y las universidades (Khoirunnisa et al., 2025). La ambición de China se refleja en sus planes quinquenales y en iniciativas como "Made in China 2025", que buscan transformar su economía hacia la alta tecnología (IntSights, 2020).

- Tipos de ciberarmas: China es conocida por sus capacidades de ciberespionaje masivo para la obtención de secretos de estado y propiedad intelectual. Los grupos de amenazas

persistentes avanzadas (APT, por sus siglas en inglés) vinculados al gobierno chino han sido responsables de campañas de espionaje a gran escala dirigidas a docenas de países e industrias, con un enfoque en la IA y el aprendizaje automático para obtener ventajas militares y de mercado (IntSights, 2020). Además, ha desarrollado ciberarmas con capacidad de sabotaje. El documento "El ciberespacio como zona de control geopolítico..." subraya la "carrera" entre China y EE. UU. por el dominio tecnológico en áreas como el 5G, lo que demuestra que la competencia estratégica se manifiesta a través de empresas privadas como Huawei (Rivas, 2021).

- Objetivos estratégicos: Sus objetivos son la disuasión estratégica y la acumulación de poder tecnológico y económico (Khoirunnisa et al., 2025). La disuasión opera a través de la demostración de sus capacidades (poder de castigo) y la inversión masiva en defensas (poder de negación). El documento Dark Side of China.pdf también menciona el uso de tecnologías de vigilancia y la censura en línea para la supresión digital de opiniones que contradicen al Partido Comunista Chino, lo que amplía sus objetivos estratégicos más allá de la mera disuasión militar (IntSights, 2020).

- Lecciones para Colombia: El modelo chino resalta la importancia de la inversión en talento humano y el ecosistema de innovación local como pilares de una estrategia de seguridad nacional a largo plazo, y muestra los riesgos de la dependencia tecnológica en la cadena de suministro.

https://www.escenariomundial.com/2025/05/23/informe-del-pentagono-expone-la-rapida-expansion-militar-de-china-y-la-amenaza-que-representa-a-ee-uu/

4.4. Israel: Disuasión Asimétrica y Modelo de Innovación

Israel, como un estado con un entorno de amenazas asimétricas, ha desarrollado una estrategia de ciberseguridad que lo ha convertido en un líder global (IISS, 2023; Khoirunnisa et al., 2025). Su modelo se basa en una estrecha colaboración entre el sector militar (Unidad 8200), la industria tecnológica y el gobierno (IISS, 2023).

- Tipos de ciberarmas: La operación Stuxnet contra las instalaciones nucleares de Irán es el ejemplo más conocido, demostrando una capacidad quirúrgica de cibersabotaje con efectos cinéticos.

- Objetivos estratégicos: El objetivo principal es la disuasión asimétrica. Israel utiliza ciberarmas no solo para defenderse, sino también para proyectar poder y disuadir a sus adversarios de emprender acciones contra sus intereses (IISS, 2023).

- Lecciones para Colombia: El caso israelí muestra que la falta de recursos de una superpotencia puede ser compensada con un modelo de innovación enfocado y una integración profunda entre los sectores público y privado, lo que es de alta relevancia para el contexto colombiano.

Infografía de la imagen de una Unidad 8200 de Israel, un"ciberdomo" que representa la defensa de la infraestructura crítica
https://www.elmundo.es/economia/2021/08/03/61030746fc6c83c7718b4593.html

5. Discusión

El estudio comparado de las potencias cibernéticas globales —Estados Unidos, Rusia, China e Israel— confirma que el desarrollo y empleo de ciberarmas se ha transformado en un elemento central de la competencia estratégica contemporánea. Dichas capacidades permiten generar efectos asimétricos a un costo relativamente bajo, ofreciendo la posibilidad de proyectar influencia política, degradar infraestructuras críticas y condicionar el comportamiento de adversarios en escenarios de confrontación híbrida (Stevens, 2017; Stoddart, 2024). Sin embargo, los mismos casos también evidencian las limitaciones de estas herramientas: el ataque NotPetya, atribuido a Rusia, ilustra cómo un ciberataque diseñado con fines militares puede producir efectos colaterales globales, con consecuencias diplomáticas y económicas para el propio agresor (Stoddart, 2024). Esta dualidad pone de relieve que las ciberarmas no constituyen un sustituto absoluto del poder convencional, sino un complemento estratégico que debe gestionarse bajo marcos de control y atribución sólidos.

En términos de sostenibilidad, la literatura enfatiza que la disuasión cibernética solo puede ser efectiva si se apoya en tres dimensiones críticas. Primero, la gobernanza internacional: los Estados requieren marcos regulatorios claros que garanticen el cumplimiento de normas jurídicas y el respeto al derecho internacional humanitario, especialmente en torno a la proporcionalidad y la protección de infraestructuras críticas (Mačák, Dias & Kasper, 2025). Segundo, la integración doctrinal: el valor de las ciberarmas se potencia cuando estas se incorporan a esquemas de operaciones conjuntas y multidominio, como lo demuestra la experiencia de la Fuerza de Apoyo Estratégico de China o la doctrina de “defender hacia adelante” en Estados Unidos (Khoirunnisa et al., 2025; IISS, 2025). Tercero, el capital humano especializado: el talento técnico constituye el verdadero núcleo de la superioridad cibernética, pero también el recurso más vulnerable frente a la competencia del sector privado (IISS, 2025).

En el caso colombiano, el Ejército, la Armada y la Fuerza Aeroespacial enfrentan un escenario en el que el ciberespacio constituye un dominio de oportunidad estratégica. A diferencia de los altos costos que implica el desarrollo de capacidades cinéticas tradicionales, las operaciones cibernéticas ofrecen ventajas costo-efectivas para el cumplimiento de la misión, particularmente en los ámbitos de fuegos habilitados por ciber, protección de redes y sistemas críticos e inteligencia de señales y ciberespionaje (Elicit, 2023; Stroppa, 2023). Estas capacidades, correctamente articuladas, pueden reducir la vulnerabilidad nacional frente a actores estatales hostiles y frente a grupos armados ilegales que ya emplean tecnologías digitales para sostener sus operaciones, como el narcotráfico y el crimen organizado transnacional.

No obstante, la sostenibilidad de estas ventajas enfrenta un reto estructural: la retención de talento cibernético. Al igual que ocurre en varios países de la OTAN, las Fuerzas Militares de Colombia deben competir con salarios y condiciones laborales más atractivas en el sector privado, lo que genera una fuga recurrente de personal altamente capacitado (IISS, 2025). En este sentido, resulta crucial diseñar un esquema de incentivos diferenciados, que incluya bonos económicos de permanencia, programas de certificación internacional y planes de carrera flexibles, para garantizar que la inversión en formación no se traduzca en capacidades perdidas para la defensa nacional.

Otro punto crítico en la discusión es la relación entre el Estado y el sector privado. Mientras que las alianzas público-privadas son esenciales para desarrollar resiliencia en infraestructuras críticas y acelerar la innovación, estas también plantean riesgos de dependencia tecnológica y concentración de poder corporativo. La literatura sobre "tecno-capitalismo" advierte que estas dinámicas, cuando no están reguladas, tienden a favorecer los intereses del capital privado en detrimento de la autonomía estatal (Hurtado, 2025). Para Colombia, el reto consiste en equilibrar la cooperación estratégica con el sector privado sin comprometer la soberanía digital ni la capacidad de decisión militar.

Finalmente, la construcción de una disuasión cibernética creíble para Colombia debe considerar un enfoque integral que articule tres frentes: (i) la institucionalización de marcos normativos como el Decreto 338 de 2022, que establece lineamientos de seguridad digital y coordinación interinstitucional; (ii) la consolidación doctrinal de capacidades conjuntas ciber en la planificación operativa multidominio; y (iii) la profesionalización y retención del talento humano mediante políticas innovadoras de estímulo y permanencia. Solo bajo estas condiciones será posible convertir al ciberespacio en un pilar efectivo de la defensa multidimensional del país, evitando tanto la dependencia tecnológica como la pérdida de personal estratégico.

En suma, Colombia se encuentra en una encrucijada estratégica: el ciberespacio ofrece una oportunidad única para amplificar su poder relativo y fortalecer su capacidad de disuasión, pero la sostenibilidad de esa ventaja dependerá de decisiones políticas y militares sobre gobernanza, talento humano y cooperación equilibrada. La experiencia internacional muestra que no basta con adquirir tecnología; es imprescindible generar estructuras institucionales y humanas que garanticen el empleo legítimo, eficaz y soberano de las ciberarmas en el marco de la defensa nacional.

5.1. Implicaciones para Colombia: Ventajas estratégicas y disuasión creíble

Basado en el análisis de los casos, la respuesta es afirmativa: el desarrollo y despliegue de ciberarmas sí puede generar ventajas estratégicas sostenibles y una disuasión creíble para Colombia, siempre que se sigan ciertos principios. Las lecciones de las potencias cibernéticas son claras:

- Poder Asimétrico: Como demostró Israel, las ciberarmas permiten a países con recursos limitados compensar desventajas militares convencionales. Colombia, que opera en un entorno geopolítico complejo con amenazas de grupos multicrimen y actores transnacionales, podría utilizar ciberarmas para proyectar poder de manera selectiva y asimétrica, disuadiendo a adversarios a un costo mucho menor que el armamento tradicional.

- Disuasión por Negación: El enfoque de disuasión por negación de Estados Unidos y China es altamente relevante. En lugar de centrarse únicamente en la capacidad de castigar a un adversario, una estrategia colombiana debe priorizar el fortalecimiento de la ciberdefensa de sus propias infraestructuras críticas. Una red de defensas robusta que haga inútiles los ataques de un adversario es la primera línea de disuasión creíble.

- Integración Civil-Militar e Innovación: La clave del éxito de Israel y China es la profunda integración entre el sector de defensa, las empresas tecnológicas y la academia. Para Colombia, esto implica la creación de un ecosistema de innovación que fomente el talento humano, la investigación y el desarrollo de tecnologías cibernéticas autóctonas. La Fuerza Pública no puede desarrollar estas capacidades de forma aislada; la colaboración con el sector privado y las universidades es fundamental.

5.1. Implicaciones para Colombia: Ventajas estratégicas y disuasión creíble

El desarrollo y despliegue de ciberarmas en Colombia no debe ser visto únicamente como una aspiración tecnológica, sino como una necesidad estratégica. Las experiencias de Israel y China muestran que las ciberarmas son catalizadores de poder asimétrico, permitiendo que Estados con recursos limitados compensen sus desventajas frente a potencias convencionales (IISS, 2023; Khoirunnisa et al., 2025). En el caso colombiano, rodeado de amenazas híbridas —desde actores multicrimen hasta grupos insurgentes y narcoterroristas con crecientes capacidades digitales—, las ciberarmas representan una oportunidad para disuadir y neutralizar amenazas a bajo costo, maximizando el impacto estratégico de la Fuerza Pública.

La disuasión por negación, planteada por Estados Unidos y China, es particularmente relevante. En lugar de priorizar el castigo, Colombia debería consolidar defensas robustas de sus infraestructuras críticas cibernéticas y de los sistemas de mando y control de las Fuerzas Militares, de modo que los ataques enemigos se vuelvan inútiles. Este enfoque es congruente

con el principio de resiliencia estratégica que, según Valeriano y Maness (2014), constituye el núcleo de una disuasión cibernética creíble.

Adicionalmente, la integración civil-militar y la innovación tecnológica son pilares indispensables. Israel ha demostrado que el talento humano formado en unidades militares puede alimentar el ecosistema nacional de innovación tecnológica (IISS, 2023). Para Colombia, esto implica una inversión decidida en formación especializada, retención de talento mediante incentivos competitivos y en la creación de un ecosistema propio de investigación y desarrollo en ciberseguridad. Sin embargo, el riesgo crítico radica en que el sector privado internacional atrae a profesionales altamente capacitados de las Fuerzas Militares, debilitando su sostenibilidad. Aquí, medidas como un bono de permanencia cibernética y planes de carrera flexibles serían instrumentos indispensables para evitar la fuga de cerebros estratégicos (IISS, 2025).

Un punto adicional es la necesidad de independencia tecnológica. La dependencia excesiva de software y hardware extranjeros, como lo evidencian los debates sobre 5G y Huawei en la geopolítica global, puede comprometer la soberanía digital y la seguridad operacional (Rivas, 2021; Hurtado, 2025). Colombia debe avanzar hacia el desarrollo de capacidades autóctonas, al menos en herramientas críticas como malware controlado para pruebas de red, sistemas de comando y control y capacidades de ciberinteligencia, de manera que se garantice la soberanía en el uso de ciberarmas y se reduzca la vulnerabilidad frente a la manipulación externa.

5.2. El marco normativo y estratégico de Colombia: Hacia la ciberdefensa

Colombia cuenta con avances normativos importantes en ciberseguridad y ciberdefensa: el CONPES 3701 (2011) reconoció por primera vez el ciberespacio como un dominio de seguridad nacional; el CONPES 3854 (2016) profundizó en la protección de infraestructuras críticas; el CONPES 3975 (2019) formalizó la política de confianza digital; y el Decreto 338 de 2022 estableció un marco de gobernanza y coordinación en seguridad digital. Finalmente, la *Política de Seguridad, Defensa y Convivencia 2022-2026* elevó la ciberdefensa a prioridad estratégica (Ministerio de Defensa Nacional, 2023).

No obstante, estas disposiciones aún resultan insuficientes. El empleo de ciberarmas requiere un marco jurídico específico y robusto, análogo al de la inteligencia (Ley 1621 de 2013), que establezca:

1. Competencias claras para las Fuerzas Militares en el ciberespacio, diferenciando funciones defensivas, ofensivas y de inteligencia.

2. Reglas de enfrentamiento cibernético (ROE-Cyber) compatibles con el Derecho Internacional Humanitario y con el Manual de Derecho Operacional de las FF.MM.
3. Mecanismos de control democrático que equilibren el secreto operativo con la rendición de cuentas.
4. Incentivos para el desarrollo tecnológico nacional, integrando a la industria de defensa con la academia y el sector privado.

La ausencia de este marco limita la legitimidad y eficacia de las operaciones cibernéticas. Como advierten Reinhold y Reuter (2023), la falta de marcos de gobernanza en el ámbito cibernético aumenta el riesgo de escaladas no controladas y de abusos de poder. Para Colombia, un marco legal robusto no solo blindaría la legitimidad del uso de ciberarmas, sino que permitiría alinear capacidades operativas con valores democráticos.

5.3. La centralidad del desarrollo de ciberarmas en la Fuerza Pública

Las ciberarmas deben consolidarse al interior de las Fuerzas Militares, no como un apéndice tecnológico aislado, sino como un componente central de su doctrina operativa. La integración de operaciones cibernéticas ofensivas (OCO) y defensivas (DCO) en los planes de campaña es fundamental para complementar fuegos, inteligencia y maniobras en dominios convencionales (Parker, 2014; US Air Force, 2023). De hecho, estudios recientes advierten que los ejércitos que no integren capacidades cibernéticas quedarán en clara desventaja frente a adversarios estatales y no estatales (Stoddart, 2024).

Para Colombia, esto implica que la Escuela Superior de Guerra y los centros de formación militar deben asumir el liderazgo en la profesionalización de oficiales y suboficiales en ciberdefensa, incluyendo certificaciones internacionales y simulaciones operacionales bajo marcos como el MITRE ATT&CK (CISA, 2021). La independencia tecnológica y la soberanía digital no pueden delegarse al sector privado; requieren estructuras militares estables, con continuidad y capacidad de innovación interna.

Grafico de barra que muestra el aumento de los delitos cibernéticos en Colombia durante 2021 y 2022., fuente Policía Nacional https://www.larepublica.co/empresas/educacion-agencias-de-gobiernos-y-salud-los-sectores-que-mas-reciben-ciberataques-4072971

5.3. El marco legal de las ciberoperaciones en Colombia: La necesidad de una Ley de Inteligencia

La naturaleza de las ciberoperaciones y el uso de ciberarmas, por sus características de invisibilidad, velocidad y dificultad de atribución, requieren un marco legal que, si bien permita su uso estratégico, garantice un control estricto para evitar abusos. En este sentido, una ley de inteligencia como la Ley 1621 de 2013 se presenta como el instrumento idóneo para cobijar estas operaciones. Su finalidad es la de fortalecer el "Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal" (Congreso de la República, 2013).

Las operaciones cibernéticas ofensivas (OCO), que buscan minimizar, neutralizar o desmantelar amenazas, se basan en la recolección de información que, por su naturaleza, debe ser tratada bajo reserva. La Ley 1621 proporciona los mecanismos para que la inteligencia cibernética opere en total secreto, protegiendo las fuentes y los métodos, pero al mismo tiempo establece una vigilancia rigurosa a través de organismos de control de la Fuerza Pública, garantizando la protección de los derechos fundamentales. Este equilibrio entre el secreto operativo y el control democrático es esencial para la legitimidad del uso de ciberarmas.

Estas herramientas son particularmente útiles para enfrentar las amenazas que se detallan en el marco de seguridad colombiano:

- Amenazas multicrimen y transnacionales: Las ciberarmas pueden ser utilizadas para obtener inteligencia sobre las estructuras de mando y control de estos grupos, sus fuentes de financiación y sus redes logísticas, permitiendo a la Fuerza Pública neutralizarlos de manera más efectiva.

- Amenazas de naturaleza cibernética: El uso de ciberarmas defensivas (DCO) es vital para proteger la infraestructura crítica nacional y los sistemas de la Fuerza Pública de ciberataques de alta sofisticación, garantizando la continuidad de las operaciones.

- Terrorismo y amenazas internas: Las capacidades de ciberinteligencia son fundamentales para identificar, monitorear y neutralizar a estos actores antes de que sus planes se materialicen, lo que fortalece la prevención y la seguridad nacional.

6. Conclusión

Este estudio ha demostrado que el desarrollo de ciberarmas sí puede generar ventajas estratégicas sostenibles y una disuasión creíble para un país como Colombia, siempre que se sigan los principios estratégicos y doctrinales correctos. A través de un análisis comparativo de las potencias cibernéticas, hemos extraído lecciones fundamentales que son directamente aplicables al contexto colombiano, superando el vacío de investigación y doctrina existente en el país.

Nuestra investigación ha revelado que la naturaleza asimétrica del ciberespacio permite a estados como Colombia compensar las desventajas militares tradicionales, proyectando poder de manera selectiva y a menor costo. La clave para una disuasión creíble no reside únicamente en las capacidades ofensivas, sino en el fortalecimiento de la ciberdefensa de la infraestructura crítica nacional, haciendo que los ataques sean inútiles para los adversarios, un principio central de la disuasión por negación.

La revisión del marco normativo colombiano, con sus CONPES y decretos, confirma que el país ha madurado en su entendimiento de las amenazas cibernéticas, transitando de la ciberseguridad a una visión más estratégica de la ciberdefensa. Sin embargo, el principal hallazgo es que la legitimidad y efectividad de estas operaciones ofensivas y defensivas dependen de un marco legal riguroso. En este sentido, proponemos que la Ley 1621 de 2013 (Ley de Inteligencia) es el vehículo idóneo para cobijar las ciberoperaciones, permitiendo el secreto operativo necesario para la inteligencia cibernética, pero garantizando al mismo tiempo el control democrático por parte de los entes de control para evitar abusos. Esta combinación de capacidad técnica y gobernanza legal es el pilar de una estrategia de ciberarmas legítima y efectiva.

Finalmente, este artículo cierra una brecha crítica en la literatura al ofrecer un modelo conceptual y recomendaciones pragmáticas para que Colombia pueda articular una estrategia nacional de ciberarmas. Las líneas de acción deben centrarse en la integración civil-militar a través de alianzas con la academia y el sector privado para fomentar el talento humano y la innovación tecnológica. Sin embargo, el camino no está exento de desafíos, como el riesgo de escalada y la proliferación de ciberarmas, que requieren una diplomacia cibernética activa y el compromiso con la creación de normas internacionales. Este estudio sienta las bases para futuras investigaciones sobre cómo un estado de segundo orden puede navegar la compleja geopolítica del ciberespacio, convirtiendo sus vulnerabilidades en una fuente de poder asimétrico y disuasión.

Referencias

Argumosa, J. (2022). Impacto del ciberespacio en las guerras del siglo XXI. En Revista del Ejército de Tierra Español, (972), 67-71.

Medina Ochoa, G. E. (Ed.). (2019). La Seguridad en el Ciberespacio: Un desafío para Colombia. Escuela Superior de Guerra "General Rafael Reyes Prieto".

Anuario Internacional CIDOB. (2010). Rusia. Perfil de país: Federación Rusa. CIDOB.

Bachkatov, N. (2010). La política de defensa de la Federación Rusa. En Anuario Internacional CIDOB (pp. 503-511).

Reinhold, T., & Reuter, C. (2023). Challenges for Cyber Arms Control: A Qualitative Expert Interview Study. Springer.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. Journal of Peace Research, 51(3), 347-360.

Stoddart, K. (2017). Cyberwarfare: Threats to Critical Infrastructure. Routledge.

Stoddart, K. (2022). Cyberwarfare: Threats to Critical Infrastructure. Routledge.

Stroppa, M. (2022). Autonomous Cyber Capabilities: A Primer. George Mason University.

US Air Force. (2023). AFDP 3-12, Cyberspace Operations. U.S. Air Force

Parker, K. L. (2014). El uso del ciberpoder. Military Review, 94(3), 50–59.

Rivas, S. M. (2021). El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos. Revista Relaciones Internacionales, (51), 89–108.

IISS. (2024). Impact of the Russia–Ukraine War on National Cyber Planning: A Survey of Ten Countries. The International Institute for Strategic Studies.

IISS. (2023). Cyber Capabilities and National Power: A Net Assessment. The International Institute for Strategic Studies.

Khoirunnisa, I. et al. (2025). Cyber Warfare and National Security: Modernizing Defense Strategies in the Context of China's Evolving Cyber Influence. China Quarterly of International Strategic Studies.

IntSights. (2020). The Dark Side of China: The Evolution of a Global Cyber Power. IntSights Cyber Intelligence.

Stevens, T. (2017). Cyberweapons: An emerging global governance challenge. Chatham House Report.

Mačák, K., Dias, T., & Kasper, Á. (2025). Handbook on developing a national position on international law and cyber activities: A practical guide for states. University of Exeter & NATO CCDCOE.

Elicit. (2023). Ciberarmas y estrategia militar en Colombia. Informe técnico.

Hurtado, J. (2025). Techno-capitalism and weaponization of cyberspace. Global Studies Quarterly, 5(2), ksaf031. https://doi.org/10.1093/isagsq/ksaf031

Congreso de la República de Colombia. (2013). Ley 1621 de 2013: Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones.

Ministerio de Defensa Nacional de Colombia. (2023). Política de Seguridad, Defensa y Convivencia Ciudadana. Garantías para la Vida y la Paz. 2022-2026.

Reinhold, T., & Reuter, C. (2023). Challenges for cyber arms control: A qualitative expert interview study. Journal of Cyber Policy, 8(1), 1–20.

Iasiello, L. (2018). Is Cyber Deterrence an Illusory Course of Action? Air University Press.

Mathur, R. (2025). Techno-Capitalism and Weaponization of Cyberspace. Global Studies Quarterly.

Referencias Adicionales

Álvarez Calderón, C. & Fernández-Osorio, A. (Eds.). (2018). Hacia una gran estrategia en Colombia: Construcción de política pública en seguridad y defensa. Volumen 1: La "Gran Estrategia": instrumento para una política integral en seguridad y defensa. Sello Editorial ESMIC.

Bustamante, J. A. (2022). No calientes que no sales. En Revista del Ejército de Tierra Español, (981), 30-35.

Calvo, J. L. (2022). Las operaciones militares en el ciberespacio. En Revista del Ejército de Tierra Español, (972), 78-83.

Fuente, I. (2022). La OTAN y el ciberespacio: un nuevo dominio para las operaciones. En Revista del Ejército de Tierra Español, (972), 84-91.

García-Patos, P. J. (2022). La inteligencia artificial en los nuevos escenarios de conflicto: Ucrania. En Revista del Ejército de Tierra Español, (981), 20-28.Álvarez Calderón, C. & Fernández-Osorio, A. (Eds.). (2018). *Hacia una gran estrategia en Colombia: Construcción de política pública en seguridad y defensa. Volumen 1: La "Gran Estrategia": instrumento para una política integral en seguridad y defensa*. Sello Editorial ESMIC.