Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XII Número: Edición Especial Artículo no.:66 Período: Diciembre del 2024

TÍTULO: Análisis de los riesgos híbridos en el territorio colombiano.

AUTORES:

1. Máster. Sara Patricia Quintero Cordero.
2. Est. Lotthar Andrey Mesa Vargas.
3. Est. Luis Carlos Pahuana Alfaro.

RESUMEN: Las amenazas híbridas, que combinan tácticas convencionales y no convencionales, han representado un desafío significativo para la seguridad en Colombia. El objetivo del estudio se ha encaminado en analizar y proponer estrategias operacionales y tecnológicas para contrarrestar las amenazas híbridas. Se empleó una metodología combinada, que incluyó la revisión de literatura, el análisis de datos cualitativos y cuantitativos, además de la aplicación del método AHP de Saaty, donde se evaluaron los desafíos doctrinales, operacionales y tecnológicos. El estudio reveló que la instrumentalización mediática ha sido fundamental para consolidar el control territorial de estos grupos. Se identificaron desafíos críticos en el ámbito tecnológico. Las conclusiones acentuaron la prioridad de desarrollar capacidades tecnológicas avanzadas y estrategias coordinadas para enfrentar las amenazas híbridas.

PALABRAS CLAVES: propaganda, desinformación, contrainteligencia, conflictos híbridos.

TITLE: Analysis of hybrid risks in the Colombian territory.

AUTHORS:

1. Master. Sara Patricia Quintero Cordero.
2. Stud. Lotthar Andrey Mesa Vargas.
3. Stud. Luis Carlos Pahuana Alfaro.

ABSTRACT: Hybrid threats, which combine conventional and unconventional tactics, have represented a significant challenge for security in Colombia. The objective of the study was aimed at analyzing and proposing operational and technological strategies to counter hybrid threats. A combined methodology was used, which included a literature review, qualitative and quantitative data analysis, and the application of Saaty's AHP method, where doctrinal, operational, and technological challenges were evaluated. The study revealed that media instrumentalization has been fundamental to consolidate the territorial control of these groups. Critical challenges were identified in the technological field. The conclusions emphasized the priority of developing advanced technological capabilities and coordinated strategies to confront hybrid threats.

KEY WORDS: propaganda, disinformation, counterintelligence, hybrid conflicts.

INTRODUCCIÓN.

El concepto de amenazas híbridas se refiere a la fusión de múltiples elementos en escenarios operativos, tanto convencionales como no convencionales. Estas amenazas abarcan dominios físicos, digitales e informativos con el fin de desestabilizar países y regiones (Jung et al., 2024). Combinan tácticas irregulares, actividades terroristas o criminales (VALLEJO, 2024) (Landeta & Cisneros, 2024), operaciones militares tradicionales, campañas masivas de desinformación (Cujabante Villamil et al., 2020), ciberataques e influencias políticas encubiertas (Afenyo & Caesar, 2023). El objetivo consiste en explotar las vulnerabilidades sociopolíticas y de seguridad de los Estados mediante enfoques indirectos de conflicto (Diaz et al., 2021). Este fenómeno ha sido ampliamente estudiado desde diversas disciplinas, al incluir las ciencias militares y las relaciones internacionales, al acentuar la prioridad en la evolución de la guerra y el conflicto global (Milshtein et al., 2024).

En Colombia, la política de seguridad ha integrado aspectos relacionados con estas amenazas híbridas. Esto responde tanto a las dinámicas del conflicto armado interno como a la influencia de actores no estatales (Cubides-Cárdenas et al., 2022). Estas amenazas buscan no solo debilitar a las fuerzas militares del Estado,

sino también complejizar su defensa mediante acciones deliberadas y sincronizadas (Arias Henao et al., 2022).

La combinación de ciberataques y manipulación mediática es un claro ejemplo de estas acciones para desestabilizar una nación (Ararat et al., 2023) (Díaz & Rangel, 2020). Eventos recientes, como la anexión rusa de Crimea, las elecciones estadounidenses del año 2016 y los ciberataques a Estonia en 2022, ilustran la efectividad contemporánea de estas estrategias híbridas (Szenes, 2023). Además, acentúa la dificultad de atribuir responsabilidades y la necesidad urgente de disuadir tales amenazas.

Por consiguiente, es crucial comprender los métodos, capacidades y objetivos estratégicos de estos actores; para ello, la siguiente investigación se centra en analizar y proponer estrategias operacionales y tecnológicas para contrarrestar las amenazas híbridas, así como enfocarse en la instrumentalización mediática y el control territorial por parte de insurgencias comerciales y grupos delictivos organizados en Colombia.

DESARROLLO.

Materiales y métodos.

Esta investigación empleó una metodología cualitativa y descriptiva (Zhang et al., 2023), basada en el análisis documental de la literatura académica sobre las amenazas híbridas y la respuesta del Estado colombiano para contrarrestarlas (Granikov et al., 2020). Los estudios descriptivos tienen como propósito caracterizar y especificar las propiedades de fenómenos, como las amenazas híbridas, con el fin de comprender su naturaleza, manifestaciones e impacto en la seguridad estatal.

AHP de SAATY.

El Proceso Analítico Jerárquico (AHP), desarrollado por Thomas Saaty en 1980, es una técnica matemática ampliamente utilizada para la toma de decisiones multicriterio. En el análisis de la contención de amenazas híbridas, el AHP se presenta como una herramienta para priorizar desafíos estratégicos en un entorno complejo y multidimensional. Este método estructura los problemas en una jerarquía que incluye un objetivo principal, como la contención eficaz de las amenazas híbridas, criterios intermedios, como los desafíos específicos identificados, y alternativas de decisión en el nivel inferior.

El AHP permite desglosar los desafíos de seguridad en componentes más manejables, al cuantificar elementos de medición, como los factores operativos y estratégicos (Akmaludin et al., 2023). El proceso se basa en varias etapas, donde la formulación del problema de la toma de decisiones en una estructura jerárquica se considera la principal (Patnaik et al., 2020). Esta etapa es donde el tomador de decisiones debe desglosar el problema en sus componentes relevantes. La jerarquía básica está compuesta por metas u objetivos generales, criterios y alternativas. La jerarquía está construida de manera que los elementos sean del mismo orden de magnitud y puedan relacionarse con algunos del siguiente nivel (figura 1).

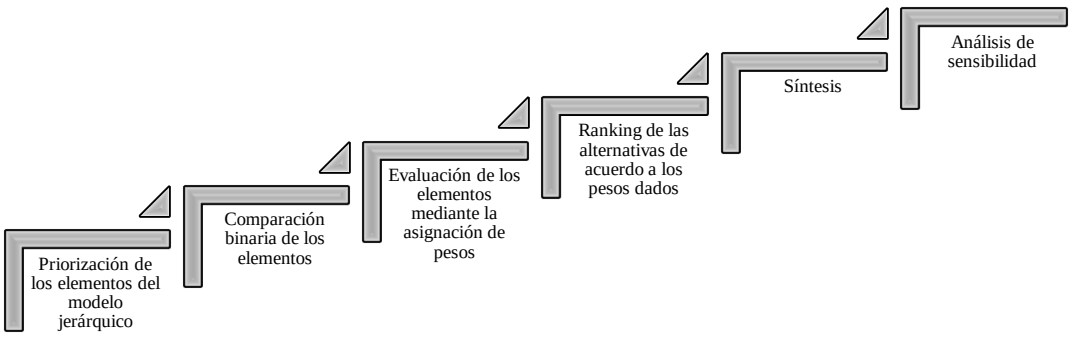

Figura 1. Metodología AHP de Saaty. Fuente: Elaboración propia.

En este caso, el método fue aplicado para determinar el peso relativo de cada desafío identificado en la contención de amenazas híbridas en Colombia. Los desafíos, que incluían aspectos como la adaptación de la doctrina militar y la seguridad cibernética, fueron jerarquizados para identificar cuáles deben ser priorizados en la planificación estratégica; por consiguiente, se evalúa cada criterio (desafío) en relación con los demás. Se asigna un valor entre 1 y 9 según la escala de Saaty, donde:

- 1: Igual importancia.
- 3: Moderada importancia de un criterio sobre otro.
- 5: Fuerte importancia.
- 7: Muy fuerte importancia.
- 9: Importancia extrema.

A continuación, se presenta un algoritmo para el cálculo de todos los criterios:

- Para cada línea de la matriz de comparación por pares determinar una suma ponderada con base a la suma del producto de cada celda por la prioridad de cada alternativa o criterio correspondiente (Carra et al., 2023).
- Para cada línea, dividir su suma ponderada por la prioridad de su alternativa o criterio correspondiente.
- Determinar la media λ_{max} del resultado de la etapa anterior.
- Calcular el índice de consistencia (CI) para cada alternativa o criterio (1).

$$CI = \frac{\lambda_{max} - m}{m - 1} \qquad (1)$$

Donde m es el número de alternativas.

- Determinar el Índice Aleatorio (IA) de la tabla 1.
- Determinar el índice de cociente de consistencia (la razón entre el índice de consistencia y el índice aleatorio).

Tabla 1. Índice aleatorio para el cálculo del coeficiente de consistencia.

Número de alternativas para la decisión n.	Índice aleatorio	Número de alternativas para la decisión n.	Índice aleatorio
3	0.58	7	1.32
4	0.9	8	1.41
5	1,12	10	1,49
6	1,24		

Fuente: Elaboración propia.

Resultados.

Las amenazas híbridas representan un desafío contemporáneo que fusiona tácticas convencionales e irregulares en conflictos, al combinar medios militares, civiles, legales e ilegales, con un enfoque en operaciones psicológicas y desinformación. Estas amenazas se caracterizan por su capacidad para explotar vulnerabilidades estatales a través de ataques cibernéticos, manipulación de información y otras formas de agresión indirecta.

En Colombia, la preparación para enfrentar estas amenazas ha requerido la integración de estrategias que aborden tanto los aspectos tecnológicos como los psicosociales. La dificultad para identificar y atribuir estas amenazas complica la respuesta estatal, debido que la naturaleza de estos conflictos desafía las formas tradicionales de guerra y el marco legal internacional; además, las amenazas híbridas difuminan los objetivos políticos y crean confusión, al complicar la toma de decisiones y la gobernabilidad. En respuesta, se han propuesto técnicas específicas para enfrentar este tipo de amenazas en Colombia, basadas en la comprensión de su compleja naturaleza.

Instrumentalización Mediática en Estrategias Híbridas.

La instrumentalización del entorno mediático y las redes sociales por parte de insurgencias comerciales y grupos delictivos organizados ha tenido un impacto en la estrategia híbrida de estos actores. Esta táctica les ha permitido expandir y consolidar su control territorial y social, al tiempo que desafían la autoridad del Estado y de las fuerzas de seguridad.

Ampliación del alcance y la influencia.

Las redes sociales y los medios de comunicación son herramientas clave para difundir propaganda, reclutar nuevos miembros y mantener la cohesión dentro de los grupos. Estas plataformas les permiten llegar a audiencias globales, difundir sus ideologías y establecer una presencia en diversas comunidades, muchas veces sin necesidad de una presencia física directa.

Desinformación y manipulación.

Las insurgencias y grupos delictivos utilizan las redes sociales para propagar noticias falsas y desinformación, al generar confusión y al debilitar la confianza en las instituciones estatales. Esta manipulación de la información dificulta la respuesta del Estado y divide a la opinión pública, al debilitar la cohesión social y la legitimidad del gobierno.

Movilización rápida y coordinada.

Estos actores utilizan las redes para coordinar acciones en tiempo real, al permitir la movilización rápida y eficiente de sus fuerzas. Esta capacidad de respuesta inmediata aumenta la letalidad de sus operaciones y hace más difícil la labor de las fuerzas de seguridad para prever y neutralizar amenazas.

Generación de recursos y legitimidad.

Estos grupos utilizan redes sociales para promover negocios ilícitos y conectar con otros actores delictivos; además, buscan legitimarse ante las comunidades locales como proveedores de seguridad o servicios, al aprovechar la ausencia o debilidad del Estado.

La instrumentalización del entorno mediático y las redes sociales ha transformado la dinámica de las insurgencias comerciales y grupos delictivos organizados, al fortalecer en la capacidad de desafiar al Estado y de consolidar su control sobre territorios y poblaciones. Esta realidad exige que las fuerzas de seguridad refuercen la ciberdefensa, la inteligencia y la comunicación estratégica para contrarrestar efectivamente estas amenazas.

Desafíos Híbridos.

Las fuerzas militares y policiales enfrentan diversos desafíos doctrinales, operacionales y tecnológicos en la contención de las amenazas híbridas. Estos desafíos emergen debido a la naturaleza multifacética y cambiante de las amenazas híbridas, que combinan elementos convencionales y no convencionales en un entorno altamente dinámico (ver tabla 2).

Tabla 2. Desafíos doctrinales, operacionales y tecnológicos en la contención de amenazas híbridas.

Tipo de desafío	Código	Desafío específico	Descripción
Doctrinales.	D1	Insuficiente adaptación de la doctrina militar.	Integración de nuevas estrategias: Las doctrinas tradicionales, centradas en conflictos convencionales, deben adaptarse para incorporar estrategias que aborden la combinación de tácticas convencionales y no convencionales. Esto incluye la integración de operaciones psicológicas, de información y cibernéticas en la planificación y ejecución de operaciones.
	D2	Baja capacidad de respuesta.	Capacitación Continua: Las fuerzas deben actualizar sus doctrinas de manera constante para reflejar las tácticas

			emergentes asociadas con las amenazas híbridas; por tanto, es esencial promover la formación continua y realizar simulaciones que permitan enfrentar escenarios complejos y en constante cambio.
	D3	Coordinación multidimensional.	Sinergia de agencias: La doctrina debe fomentar una mayor coordinación entre diferentes agencias gubernamentales y sectores de la sociedad civil para enfrentar las amenazas híbridas de manera integral.
Operacionales.	O1	Complejidad del entorno de operaciones.	Ambiente volátil e incierto: Las amenazas híbridas crean un entorno de operaciones que es incierto, ambiguo y complejo, al dificultar la identificación y evaluación de amenazas en tiempo real.
	O2	Multidimensionalidad de las amenazas.	Respuesta sincronizada: Las fuerzas deben desarrollar la capacidad para responder a amenazas que operan simultáneamente en diferentes dimensiones (cibernética, física, psicológica), al requerir una coordinación efectiva y la implementación de estrategias diversificadas.
	O3	Desinformación y manipulación.	Contramedidas psicológicas: Enfrentar la desinformación y la manipulación de medios requiere estrategias avanzadas de contramedidas psicológicas y de información para mitigar su impacto en la percepción pública y en la moral de las fuerzas.
Tecnológicos.	T1	Ataques cibernéticos.	Protección de infraestructura: La protección de las redes y sistemas de comunicación frente a ataques cibernéticos es objetiva. Los grupos híbridos suelen emplear técnicas avanzadas de hacking y ciberespionaje, al exigir medidas de mayor seguridad cibernética.
	T2		Adopción de nuevas tecnologías: Las fuerzas deben mantenerse al día con los avances tecnológicos en el ámbito de la ciberdefensa, la vigilancia y la recopilación de inteligencia. Esto incluye la implementación de herramientas de análisis de datos y sistemas de inteligencia artificial para detectar y neutralizar amenazas emergentes.
	T3	Interoperabilidad de sistemas	Integración tecnológica: La interoperabilidad entre diferentes plataformas y sistemas tecnológicos es transcendental para una respuesta efectiva. Esto implica la integración de tecnologías de comunicación, vigilancia y análisis para proporcionar una visión coherente y coordinada de las amenazas.

Fuente: Elaboración propia.

Una vez identificados los desafíos, se propone implementar la modelación del método AHP de Saaty, que permite priorizar los desafíos en la contención de amenazas híbridas (ver tabla 3 y 4); por consiguiente, se procede a evaluar y comparar los diversos factores que afectan la seguridad nacional, al facilitar la identificación y priorización de los desafíos clave.

Tabla 3. Matriz normalizada según AHP de Saaty.

Criterios	D1	D2	D3	O1	O2	O3	T1	T2	T3	PESO
D1	0.07	0.04	0.06	0.06	0.13	0.09	0.12	0.08	0.04	0.07
D2	0.05	0.02	0.02	0.02	0.03	0.02	0.12	0.08	0.02	0.04
D3	0.07	0.04	0.03	0.03	0.06	0.04	0.12	0.08	0.02	0.05
O1	0.05	0.02	0.02	0.02	0.01	0.01	0.03	0.08	0.09	0.04
O2	0.07	0.04	0.03	0.03	0.02	0.02	0.01	0.04	0.04	0.03
O3	0.10	0.07	0.12	0.06	0.13	0.18	0.03	0.08	0.09	0.09
T1	0.40	0.56	0.36	0.45	0.25	0.27	0.23	0.24	0.35	0.35
T2	0.10	0.14	0.24	0.23	0.19	0.18	0.17	0.16	0.17	0.18
T3	0.10	0.07	0.12	0.11	0.19	0.18	0.17	0.16	0.17	0.14

Fuente: Elaboración propia.

Tabla 4. Análisis de la consistencia según AHP de Saaty.

Criterios		Valores propios aproximados	
D1	0.78	10.42377745	
D2	0.42	9.90430463	
D3	0.55	10.11084113	Valor propio= 10.1207
O1	0.34	9.359940813	IC=0.14
O2	0.32	9.740288729	RC=0.10<=0.10
O3	0.98	10.34152201	Consistente.
T1	3.59	10.36166941	
T2	1.85	10.50742125	
T3	1.47	10.33656922	

Fuente: Elaboración propia.

En el contexto colombiano, el Ejército Nacional, a través del Manual de Técnicas Contra Amenazas Hibridas de Colombia (en adelante MTCAH), ha desarrollado estrategias para contrarrestar las amenazas híbridas, que combinan tácticas convencionales y no convencionales, así como actividades criminales y terroristas. Estas amenazas se caracterizan por su naturaleza deliberada, sincronizada y coordinada, y requieren un enfoque operativo integral que involucra la cooperación con agencias gubernamentales y actores multinacionales.

Según los resultados obtenidos del método AHP de Saaty determina que los ataques cibernéticos (peso =0.34), la desactualización ante las tecnologías emergentes (peso=0.18) y la interoperabilidad de sistemas (peso=0.14), coinciden con las prioridades estratégicas discutidas en el análisis de las amenazas híbridas. En este caso, el MTCAH destaca la necesidad de actividades de estabilidad y operaciones unificadas para mantener la seguridad en un ambiente volátil y complejo. Incluso, las amenazas híbridas, como ataques cibernéticos, desinformación y sabotaje ambiental, desafían la gobernabilidad y estabilidad social, especialmente en regiones vulnerables.

El enfoque operacional del Ejército colombiano incluye la "Acción Integral", que busca mitigar la influencia de insurgencias comerciales que emplean coerción, violencia y manipulación de información para desafiar la seguridad del Estado. Este enfoque integral incluye la adaptación a escenarios híbridos, donde la información y las decisiones estratégicas son críticas.

Finalmente, las amenazas híbridas en Colombia han generado una evolución en las modalidades de operación militar, que ahora deben abordar las complejidades y ambigüedades de estos conflictos. La interacción entre grupos insurgentes y la sociedad ha dificultado la distinción entre combatientes y civiles, al complicar aún más la respuesta estatal; por tanto, se deben proponer acciones específicas para mitigar su impacto, al comenzar con los desafíos de mayor incidencia en conjunto con las de menor peso; para ello, se propone un marco operativo integrado para potenciar las acciones en función de mitigar las amenazas híbridas.

Marco Operativo Integrado para Mitigar Amenazas Híbridas.

El entorno de seguridad actual, caracterizado por la naturaleza híbrida de las amenazas, requiere un enfoque operativo multiobjetivo que integre ciberdefensa, manejo de la información, inteligencia y contrainteligencia, y acción integral. Este marco operativo busca consolidar estos elementos en una estrategia cohesiva que permita a las fuerzas militares y policiales responder ante las amenazas híbridas (ver tabla 5).

Tabla 5. Componentes y estrategias del marco operativo.

Componente	Objetivo	Estrategias
Ciberdefensa.	Proteger infraestructuras críticas y redes de comunicación contra ataques cibernéticos, un componente clave en estrategias de actores híbridos.	▪ Detección y respuesta temprana: Implementar sistemas avanzados de monitoreo y alerta temprana para identificar amenazas cibernéticas en tiempo real. ▪ Protección de infraestructura crítica: Desarrollar y mantener medidas de seguridad cibernética. ▪ Capacitación y preparación: Entrenar a personal especializado y realizar simulaciones periódicas.
Manejo de la información.	Controlar y dirigir la narrativa en el entorno mediático y redes sociales, al contrarrestar la propaganda y desinformación.	▪ Monitoreo y análisis de redes sociales: Establecer unidades de monitoreo continuo. ▪ Desarrollo de narrativas efectivas: Crear mensajes claros y coherentes. ▪ Educación y concienciación pública: Implementar programas educativos para fortalecer la capacidad de discernimiento.
Inteligencia y contrainteligencia.	Obtener y analizar información relevante para anticipar y neutralizar acciones de actores híbridos, al proteger las operaciones propias.	▪ Integración de inteligencia multidimensional: Fomentar colaboración interagencial. ▪ Operaciones de contrainteligencia: Identificar y neutralizar infiltraciones. ▪ Uso de tecnología avanzada: Implementar herramientas tecnológicas de última generación.
Acción integral	Coordinar esfuerzos civiles y militares para un enfoque unificado y eficaz en la respuesta a amenazas híbridas.	▪ Colaboración interagencial: Establecer mecanismos de cooperación entre fuerzas armadas, agencias y actores civiles. ▪ Participación comunitaria: Involucrar a la comunidad en estrategias de seguridad. ▪ Acciones de estabilización: Implementar operaciones que busquen neutralizar amenazas y estabilizar regiones afectadas.

Fuente: Elaboración propia.

Fases de implementación del marco operativo:

- Evaluación inicial: Realizar un diagnóstico de las capacidades actuales y las necesidades operativas para enfrentar amenazas híbridas.
- Desarrollo de capacidades: Fortalecer las áreas identificadas como críticas, mediante la inversión en tecnología, capacitación y el desarrollo de nuevas doctrinas operativas.

- Integración y coordinación: Establecer centros de comando y control que integren las operaciones de ciberdefensa, manejo de la información, inteligencia y contrainteligencia, y acción integral.
- Monitoreo y evaluación: Implementar un sistema de seguimiento y evaluación continuo para ajustar las estrategias y tácticas en función de la evolución de las amenazas.

Estrategias Integrales de Monitoreo y Comunicación para Amenazas Híbridas.

Estas estrategias buscan integrar tecnología avanzada, colaboración intersectorial y una sólida capacidad de respuesta comunicacional para enfrentar las amenazas híbridas; por consiguiente, se proponen las siguientes estrategias, que incluyen el monitoreo de redes sociales y el análisis de la comunicación estratégica:

1. Plataforma integral de monitoreo de redes sociales.
   - Desarrollo de un sistema automatizado: Implementar una plataforma que utilice inteligencia artificial (IA) para monitorear, en tiempo real, actividades sospechosas en redes sociales. De modo que se detecte patrones de comportamiento, palabras clave y tendencias relacionadas con amenazas híbridas.
   - Análisis predictivo: Aplicar algoritmos de aprendizaje automático para predecir posibles amenazas basadas en el análisis de datos históricos y actuales, al permitir una respuesta proactiva.
2. Unidad de respuesta rápida en comunicación estratégica.
   - Creación de equipos especializados: Formar unidades especializadas en la creación de narrativas estratégicas, capaces de contrarrestar desinformación y propaganda, al difundir información veraz de manera rápida y efectiva en las plataformas más relevantes.
   - Uso de bots y algoritmos de amplificación: Desarrollar y desplegar bots que amplifiquen mensajes oficiales y contrarresten la desinformación, al asegurar que las narrativas oficiales alcancen una mayor audiencia.
3. Programa de colaboración multisectorial.

- Alianzas con empresas tecnológicas: Establecer alianzas con empresas de redes sociales y tecnología para el intercambio de información y desarrollo de herramientas conjuntas que permitan una mejor detección y eliminación de contenido malicioso.
- Red de colaboración comunitaria: Crear una red de colaboración con organizaciones civiles y comunidades locales para reportar actividades sospechosas y fortalecer la resiliencia social frente a las amenazas híbridas.

4. Laboratorio de análisis de comunicación estratégica.

- Análisis de sentimientos y opinión pública: Implementar técnicas avanzadas de análisis de sentimientos para evaluar el impacto de las narrativas enemigas y ajustar las estrategias de comunicación en consecuencia.
- Simulación de escenarios: Desarrollar simulaciones de escenarios de crisis híbrida para entrenar a los equipos de comunicación en la gestión de crisis, al asegurar respuestas rápidas y coherentes.

5. Capacitación continua y adaptativa.

- Programas de formación en nuevas tecnologías: Establecer programas de formación continua para el personal militar y policial en el uso de nuevas tecnologías de monitoreo y análisis, al asegurar que estén siempre a la vanguardia.
- Educación a la población: Implementar campañas educativas para aumentar la conciencia pública sobre las amenazas híbridas y cómo identificarlas, al reducir la vulnerabilidad de la sociedad a la desinformación.

Por último, se han propuesto a desarrollar dos proyectos estratégicos para enfrentar los desafíos en resiliencia mediática y ciberdefensa en Colombia. Estos proyectos se encuentran diseñados para mejorar la capacidad de respuesta ante amenazas híbridas y reforzar la seguridad territorial (ver tabla 6).

Tabla 6. Proyectos para la resiliencia mediática y ciberdefensa en Colombia.

Característica	**Proyecto 1:** Fortalecimiento de la resiliencia mediática y territorial en Colombia.	**Proyecto 2:** Ciberdefensa y comunicación estratégica para la seguridad territorial.
Alcance	Creación de una red integral de resiliencia mediática y territorial en comunidades vulnerables de Colombia.	Desarrollo de capacidades avanzadas en ciberdefensa y comunicación estratégica para proteger el control territorial en Colombia.
Tiempo	24 meses	36 meses
Objetivo general	Desarrollar y fortalecer capacidades locales para contrarrestar la instrumentalización mediática y mejorar la gobernanza territorial.	Fortalecer las capacidades del Estado colombiano en ciberdefensa y comunicación estratégica.
Etapas	▪ Fase 1: Diagnóstico de la situación mediática y territorial. ▪ Fase 2: Desarrollo de programas de educación y capacitación. ▪ Fase 3: Implementación de la red y estrategias de recuperación territorial. ▪ Fase 4: Monitoreo y evaluación de las intervenciones.	▪ Fase 1: Análisis y mapeo de vulnerabilidades en infraestructuras críticas. ▪ Fase 2: Desarrollo e implementación de un sistema integral de ciberdefensa. ▪ Fase 3: Capacitación y despliegue de la unidad de respuesta rápida. ▪ Fase 4: Evaluación y ajuste de las estrategias.
Recursos	▪ Tecnología para monitoreo y comunicación. ▪ Materiales educativos y de capacitación. ▪ Equipos de comunicación y transporte.	▪ Infraestructura tecnológica avanzada. ▪ Herramientas y software para análisis y respuesta a ciberataques. ▪ Equipos de comunicación estratégica.
Impacto esperado	▪ Reducción de la influencia de la propaganda insurgente. ▪ Mejora en la gobernanza local. ▪ Empoderamiento comunitario.	▪ Protección de infraestructuras críticas. ▪ Respuesta rápida frente a desinformación. ▪ Mejora en la coordinación de seguridad.
Niveles de aprobación	▪ Aprobación por autoridades locales y nacionales. ▪ Supervisión por entidades de cooperación internacional.	▪ Aprobación por fuerzas armadas y gobierno nacional. ▪ Coordinación con agencias internacionales de ciberseguridad.
Financiamiento	▪ Fondos gubernamentales. ▪ Apoyo de organismos internacionales y ONGs. ▪ Contribuciones de universidades y centros de investigación.	▪ Fondos del Ministerio de Defensa. ▪ Apoyo de organismos internacionales. ▪ Contribuciones de universidades y centros de investigación.
Beneficios a alcanzar	▪ Fortalecimiento de la cohesión social en áreas vulnerables. ▪ Disminución de la influencia de insurgencias y grupos delictivos. ▪ Participación comunitaria en la defensa territorial.	▪ Protección efectiva de infraestructuras críticas. ▪ Control territorial fortalecido frente a amenazas híbridas. ▪ Coordinación eficiente entre el Estado y la academia.

Fuente: Elaboración propia.

Discusión.

En este estudio, se identificó que la instrumentalización mediática y el control territorial ejercidos por insurgencias comerciales y grupos delictivos organizados en Colombia han tenido un impacto significativo en la estabilidad social y la gobernanza local. Los datos obtenidos mostraron que las estrategias de desinformación y propaganda desplegadas por estos grupos han logrado amplificar su influencia, no solo en las zonas bajo su control, sino también en áreas circundantes.

Se observó que las fuerzas militares y policiales enfrentan desafíos significativos en términos doctrinales, operacionales y tecnológicos para contrarrestar estas amenazas híbridas. En particular, la falta de una estrategia integrada que combine ciberdefensa, manejo de la información, y acciones de inteligencia y contrainteligencia ha dificultado la capacidad de respuesta frente a las tácticas avanzadas de insurgencias y grupos delictivos. Los resultados indicaron una necesidad urgente de desarrollar capacidades en estas áreas para mitigar el impacto de estas amenazas.

Adicionalmente, la modelación del método AHP de Saaty reveló que los desafíos tecnológicos, específicamente aquellos relacionados con la ciberdefensa y la comunicación estratégica, son los que más inciden en la capacidad para contener y neutralizar las amenazas híbridas. Los resultados sugieren que la inversión en tecnologías avanzadas y la formación de personal especializado son prioritarias para mejorar la eficacia operativa en este contexto

El estudio evidenció la creciente relevancia de la instrumentalización mediática en las estrategias de insurgencias y grupos delictivos, al resaltar la necesidad de que las fuerzas de seguridad profundicen en la comprensión de las dinámicas mediáticas.

Las actuales estrategias de seguridad en Colombia presentan limitaciones, particularmente en la integración de ciberdefensa y comunicación estratégica. Los desafíos tecnológicos representados por el método AHP de Saaty indican, que se deben priorizar políticas que fortalezcan la inversión en tecnología y la formación de personal especializado para enfrentar las amenazas híbridas.

CONCLUSIONES.

La instrumentalización mediática ha sido crucial para consolidar el control territorial por parte de insurgencias comerciales y grupos delictivos organizados en Colombia.

Este estudio demostró que las estrategias de desinformación y propaganda han amplificado la influencia de estos grupos, al afectar no solo las áreas bajo su control, sino también las regiones circundantes; además, el manejo propagandístico en el entorno mediático y las redes sociales se volvió fundamental en sus estrategias híbridas; de modo que han generado desafíos inéditos para las fuerzas militares y policiales en términos doctrinales, operacionales y tecnológicos.

Los desafíos identificados evidenciaron una brecha significativa en la capacidad de respuesta frente a las amenazas híbridas. La falta de una estrategia integrada que combinara ciberdefensa, manejo de la información e inteligencia, limitó la eficacia de las fuerzas de seguridad. Este resultado resaltó la necesidad de desarrollar enfoques operativos más coordinados, con especial énfasis en la ciberdefensa y la comunicación estratégica; así como la colaboración con los centros de investigación de ciencias militares y de defensa en proyectos encaminados a fortalecer de la resiliencia mediática, la ciberdefensa y la comunicación estratégica para la seguridad territorial.

El método AHP de Saaty confirmó que los desafíos tecnológicos fueron los más influyentes en la respuesta a estas amenazas; por lo tanto, se concluyó que se debe priorizar la inversión en tecnologías avanzadas y la formación especializada del personal; además, se señaló la necesidad de que las autoridades conciban estrategias innovadoras e integrales para la contención y respuesta; de modo que aborde la *letalidad híbrida* con enfoques que integren el monitoreo de redes sociales, el análisis de comunicación estratégica, y programas específicos de ciberdefensa.

REFERENCIAS BIBLIOGRÁFICAS.

1. Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236(April), 2-7. https://www.sciencedirect.com/science/article/pii/S0964569123000182
2. Akmaludin, A., S, E. G., Rinawati, R., Arisawati, E., & Dewi, L. S. (2023). Decision Support for Selection of The Best Teachers Recommendations MCDM-AHP and ARAS Collaborative Methods. Sinkron : jurnal dan penelitian teknik informatika, 8(4), 2036-2048. https://www.polgan.ac.id/jurnal/index.php/sinkron/article/view/12354
3. Ararat, P. A. P., Ortiz, Z. X. R., Hernández, F. A. C., & Pantoja, A. H. (2023). Perfil profesional en ciberseguridad y ciberdefensa: un ejercicio exploratorio de conceptualización. Revista da UNIFA, 36, 1-15. https://revistadaunifa.fab.mil.br/index.php/reunifa/article/view/549
4. Arias Henao, D. P., Arias Henao, H. E., & García Perilla, J. C. (2022). Nueva Violencia colombiana y el rol de la fuerza pública en los escenarios de justicia transicional a 2021. Opinión Jurídica, 21(45), e3. http://www.scielo.org.co/scielo.php?pid=S1692-25302022000200003&script=sci_arttext
5. Carra, M., Botticini, F., Filippo Carlo, P., Giulio, M., Pezzagno, M., & Barabino, B. (2023). A comparative cycling path selection for sustainable tourism in Franciacorta. An integrated AHP-ELECTRE method. Transportation Research Procedia, 69(February), 451-452. https://www.sciencedirect.com/science/article/pii/S2352146523002041
6. Cubides-Cárdenas, J., González Agudelo, J. D., & Navas-Camargo, F. (2022). Key principles for the use of force in urban scenarios in Colombia. Revista Científica General José María Córdova, 20(37), 89-107. http://www.scielo.org.co/scielo.php?pid=S1900-65862022000100088&script=sci_abstract&tlng=en

7. Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (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. http://www.scielo.org.co/scielo.php?pid=S1900-65862020000200357&script=sci_arttext

8. Diaz, J. M., Staples, H., Kanai, J. M., & Lombard, M. (2021). Between pacification and dialogue: Critical lessons from Colombia's territorial peace. Geoforum, 118(January), 106-116. https://www.sciencedirect.com/science/article/pii/S001671852030289X

9. Díaz, M. O., & Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62(2), 199-217. https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/download/168/258

10. Granikov, V., Hong, Q. N., Crist, E., & Pluye, P. (2020). Mixed methods research in library and information science: A methodological review. Library & Information Science Research, 42(1), 3-6. https://www.sciencedirect.com/science/article/abs/pii/S0740818819302294

11. Jung, P. H., Thill, J.-C., & Galvis-Aponte, L. A. (2024). State fragility, violence and trade: Dangerous trade routes in Colombia. Papers in Regional Science, 103(4), 1-15. https://www.sciencedirect.com/science/article/pii/S1056819024000435

12. Landeta, A. A., & Cisneros, D. (2024). EL TERRORISMO EN ECUADOR: UN ANÁLISIS LONGITUDINAL. Revista de la Academia del Guerra del Ejército Ecuatoriano, 17(01), 10. https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/3335

13. Milshtein, D., Henik, A., Ben-Zedeff, E. H., & Milstein, U. (2024). Mind on the battlefield: what can cognitive science add to the military lessons-learned process? Defence Studies, 24(2), 277-298. https://www.tandfonline.com/doi/full/10.1080/14702436.2024.2316138

14. Patnaik, P. K., Swain, P. T. R., Mishra, S. K., Purohit, A., & Biswas, S. (2020). Composite material selection for structural applications based on AHP-MOORA approach. Materials Today: Proceedings, 33(Part 8), 5659-5663. https://www.sciencedirect.com/science/article/abs/pii/S221478532032678X

15. Szenes, Z. (2023). Reinforcing deterrence: assessing NATO's 2022 Strategic Concept. Defense & Security Analysis, 39(4), 539-560. https://www.tandfonline.com/doi/full/10.1080/14751798.2023.2270230

16. Vallejo, F. F. E. (2024). La planificación de la fuerza terrestre ecuatoriana ante la amenaza emergente del terrorismo. Revista de la Academia de Guerra del Ejército Ecuatoriano, 17(01), 10. https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/3350

17. Zhang, C., Tian, L., & Chu, H. (2023). Usage frequency and application variety of research methods in library and information science: Continuous investigation from 1991 to 2021. Information Processing and Management, 60(6), 4-8. https://www.sciencedirect.com/science/article/abs/pii/S0306457323002443

DATOS DE LOS AUTORES.

1. **Sara Patricia Quintero Cordero.** Magíster en Relaciones Internacionales de la Universidad de Buenos Aires. Docente e investigadora del grupo de Ciencias Militares de la Escuela Militar de Cadetes «General José María Córdova». (ESMIC). Colombia. E-mail: sara.quintero@esmic.edu.co

2. **Lotthar Andrey Mesa Vargas.** Estudiante de Ciencias Militares y Relaciones Internacionales de la Escuela Militar «General José María Córdova». (ESMIC). Colombia. E-mail: lotthar.mesa@esmic.edu.co

3. **Luis Carlos Pahuana Alfaro.** Estudiante de Ciencias Militares y Relaciones Internacionales de la Escuela Militar «General José María Córdova». (ESMIC). Colombia. E-mail: luis.pahuana@esmic.edu.co

RECIBIDO: 30 de septiembre del 2024. **APROBADO:** 26 de octubre del 2024.