



ESIC

ESCUELA DE INTELIGENCIA Y CONTRAINTELIGENCIA
"BRIGADIER GENERAL RICARDO CHARRY SOLANO"
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

Del campo de batalla al campo digital: Inteligencia Militar y redes sociales.

Escrito por:

Jorge Alejandro Zamorano Contreras

Abogado – Mag. Estrategia y Geopolítica

RESUMEN:

En Boyacá en 1819, controlar un puente decidió el destino de una campaña; hoy, controlar nodos de información puede condicionar percepciones, voluntades y legitimidad operacional.

La evolución de la guerra trasladó parte del combate desde el terreno físico hacia el campo digital, donde redes sociales, datos, narrativas y emociones se convierten en fuentes de inteligencia y vectores de influencia. Comprender esta transformación es esencial para anticipar amenazas, proteger la información y fortalecer la superioridad institucional en escenarios híbridos.

ANTECEDENTES

1819 – Batalla del puente de Boyacá: el control del puente físico permitió decidir una campaña. El terreno era el nodo crítico de la maniobra.

Guerras de primera a tercera generación: la guerra evolucionó de formaciones lineales y masa terrestre hacia fuego, maniobra, aviación, comunicaciones, inteligencia técnica y operaciones psicológicas.

Cuarta generación: el enemigo se vuelve difuso; desaparecen frentes definidos y se integran amenazas asimétricas, híbridas, informacionales y no convencionales.

Siglo XXI: el ciberespacio y las redes sociales ampliaron el campo de batalla hacia datos, narrativas, emociones, reputación y legitimidad.

Actualidad: el puente físico cedió paso al nodo digital; quien domina información, percepción y oportunidad decisional obtiene ventaja táctica, operacional y estratégica.



Imagen generada con IA

CONTEXTO ACTUAL

El escenario operacional contemporáneo exige que la inteligencia militar trascienda la observación del terreno físico e incorpore el entorno digital como espacio permanente de vigilancia, alerta temprana, protección de la fuerza y apoyo a la decisión. Así como en Boyacá en 1819 el control del puente permitió incidir sobre la movilidad, la maniobra y el desenlace de la campaña, hoy los nodos digitales condicionan la lectura del ambiente operacional, la seguridad de las operaciones y la legitimidad institucional.

En este marco, las redes sociales constituyen una fuente abierta de interés estratégico, pero no son inteligencia por sí mismas. Su valor surge cuando los datos son orientados, recolectados, procesados, validados, integrados y diseminados dentro del ciclo de inteligencia. La inteligencia de redes sociales (SOCMINT) debe articularse con inteligencia de fuentes abiertas (OSINT), inteligencia humana (HUMINT), inteligencia de señales (SIGINT) e inteligencia de imágenes (IMINT), bajo criterios de oportunidad, confiabilidad, trazabilidad, contraste multisensor y respaldo legal en la toma de decisiones.

La evolución hacia guerras de quinta y sexta generación —categorías aún discutidas doctrinalmente— advierte una tendencia: la confrontación se desplaza hacia dominios cognitivos, algorítmicos, espaciales, cibernéticos y psicológicos. Para Colombia, el reto no consiste en observar más, sino en interpretar mejor: detectar narrativas hostiles, anticipar riesgos, proteger información sensible, neutralizar desinformación y convertir grandes volúmenes de datos en conocimiento accionable, jurídicamente controlado y operacionalmente útil para el mando.

"EN GUARDIA POR LA PATRIA"





IMPLICACIONES

La transición del puente físico al nodo digital impone una modificación sustancial en la forma de concebir la inteligencia militar: ya no basta con identificar dónde está el adversario, sino comprender cómo se mueve (física y digitalmente), comunica, influye, oculta, distorsiona y explota el entorno informacional. Una fotografía, una transmisión en vivo, una tendencia digital o una filtración aparentemente marginal pueden revelar ubicación, intención, moral de la tropa, vulnerabilidades logísticas o percepción ciudadana frente a una operación.

Este escenario exige nuevas capacidades de análisis, validación y fusión multisensor. En las guerras de cuarta generación, el adversario opera de forma difusa, híbrida y asimétrica; en las aproximaciones de quinta generación, busca afectar percepciones, voluntades y legitimidad; y en las discusiones sobre sexta generación, la velocidad decisional se vincula con automatización, inteligencia artificial, ciberespacio y dominio informacional. Por ello, la inteligencia de redes sociales (SOCMINT) debe integrarse con inteligencia de fuentes abiertas (OSINT), inteligencia humana (HUMINT), inteligencia de señales (SIGINT) e inteligencia de imágenes (IMINT), no como acumulación de datos, sino como arquitectura de comprensión operacional.

La consecuencia directa para Colombia es la necesidad de anticipar el “efecto red” antes, durante y después de cada operación. Toda acción militar tiene el riesgo exponencial que puede ser narrada, manipulada, descontextualizada o amplificada en tiempo real. Esto exige protocolos estrictos de seguridad operacional, disciplina digital del personal, análisis de narrativas adversas, protección de información sensible y capacidad institucional para responder con oportunidad, precisión y legitimidad. En la guerra contemporánea, perder el control del relato puede reducir la libertad de acción del mando incluso cuando la operación haya sido táctica y jurídicamente correcta.

AFECTACIONES PARA COLOMBIA



Imagen generada con IA

Para Colombia, el desplazamiento del campo de batalla hacia el nodo digital genera una afectación directa sobre la libertad de acción del Estado. Las operaciones militares ya no se evalúan únicamente por sus resultados tácticos, sino por la forma en que son interpretadas, difundidas y disputadas en el espacio público. Una operación exitosa puede perder eficacia estratégica si es descontextualizada mediante narrativas hostiles, filtraciones, imágenes parciales o campañas coordinadas de desinformación.

Esta realidad impacta la seguridad operacional, la moral de la fuerza, la protección de fuentes, la reserva de inteligencia y la confianza ciudadana. En zonas donde convergen grupos armados organizados, economías ilícitas, conflictividad social y presión mediática, las redes sociales pueden ser utilizadas para anticipar movimientos de la Fuerza Pública, exponer personal, manipular comunidades, erosionar legitimidad o condicionar decisiones del mando.

La principal afectación no es tecnológica, sino estratégica: Colombia enfrenta adversarios capaces de combinar presencia territorial, intimidación social, propaganda digital y explotación política de la información. Por ello, la superioridad militar debe complementarse con superioridad informacional, disciplina digital, contrainteligencia activa, análisis de narrativas y capacidad institucional para comunicar con precisión, oportunidad y credibilidad.

En el siglo XXI, la soberanía no se protege únicamente mediante el control del territorio, sino también mediante la defensa de la verdad operacional, la integridad de la información y la legitimidad institucional. Un Estado que no comprende, monitorea y disputa el ecosistema digital corre el riesgo de obtener superioridad táctica en el terreno, mientras pierde ventaja estratégica en la percepción pública, en la narrativa dominante y en la confianza ciudadana.

REFERENCIAS

- Banco de la República. (s. f.). *Puente de Boyacá*. Congreso de Colombia. (2013). *Ley 1621 de 2013*.
Haro Ayerve, P. (2019). La guerra de cuarta generación y las amenazas asimétricas. *Política y Estrategia*, 134, 93–113. Herrick, D. F. (2016). *The social side of cyber power?* NATO CCDCOE.
Joint Chiefs of Staff. (2018). *Joint concept for operating in the information environment*. U.S. Department of Defense.
NATO. (2023). *Allied joint doctrine for information operations AJP-10.1*. NATO Standardization Office.
Omand, D., Bartlett, J., & Miller, C. (2012). *#Intelligence*. Demos.
RAND Corporation. (2017). *Monitoring social media*.