ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA: GESTIÓN DE LA INFORMACIÓN, UTILIDAD DE INTELIGENCIA DE FUENTES ABIERTAS (OSINT) Y BIG DATA.

TITULO: UTILIDAD DE LA INTELIGENCIA DE FUENTES ABIERTAS (OSINT) Y BIG DATA, PARA AGILIZAR LA GESTIÓN DE INFORMACIÓN, EN APOYO A LA TOMA DE DECISIONES EN EL NIVEL OPERACIONAL.

AUTOR: Mayor GUSTAVO ARIEL LERA.

TUTOR: Teniente Coronel DARIO LUCERO.

AÑO: 2024

Resumen

La información tiene un valor muy importante durante el proceso de toma de decisiones del comandante en las operaciones militares. Por ello, una fuerza militar que pretenda alcanzar eficiencia durante el cumplimiento de su misión deberá considerar como requisito fundamental alcanzar una correcta gestión de la información.

En la actualidad, con el desarrollo de la tecnología, es un desafío darle mejor tratamiento a la información de manera oportuna, permitiendo reducir la incertidumbre y los tiempos para adoptar una resolución y a su vez evitar la saturación/intoxicación del decisor.

Así mismo, en la era de la información, el Big Data y la inteligencia de fuentes abiertas (OSINT) han emergido como herramientas cruciales en el ámbito de la inteligencia. Estas tecnologías permiten la recolección, análisis y explotación de grandes volúmenes de datos para mejorar la toma de decisiones estratégicas y operacionales, particularmente.

Este trabajo describe y analiza la importancia de estas herramientas, para gestionar información en el proceso de inteligencia, evaluando su impacto en la eficiencia, efectividad en la toma de decisiones, en el marco del nivel operacional.

Palabras clave

Inteligencia de fuentes abiertas (OSINT) – Big Data – Proceso de Inteligencia – Información.

Tabla de Contenido

Índice de Figuras

Introducción

El uso de la información ha ido creciendo exponencialmente con el paso de los años en los conflictos armados pasando a ser un factor sustancial dentro de un teatro de operaciones. A lo largo de los años, en diferentes contiendas, su empleo ha ganado trascendencia motivado por la evolución tecnológica.

Con el advenimiento de internet, redes sociales, smartphones inteligentes, las nuevas tecnologías convirtieron a cada ciudadano en un nodo permanentemente conectado a una red global. Este fenómeno no excluyó a las operaciones militares en el campo de combate. Su alcance se amplió, afectando no solo los sistemas de comando y control y la toma de decisiones, sino también la capacidad de procesamiento de la información.

En relación con ello, la doctrina conjunta (Estado Mayor Conjunto de las Fuerzas Armadas, 2019), entiende como activo de información:

Cualquier información o componente de un sistema de información que tenga valor para una organización del Sistema de Defensa Nacional, susceptible de ser afectado deliberada o accidentalmente con consecuencias para el mismo. Los activos de información incluyen: datos, información, servicios y procesos de un sistema, software, hardware, comunicaciones, recursos materiales y recursos humanos que componen un sistema de información.

Otra acepción de la información es su identificación como un dominio. Los primeros dominios que se reconocieron fueron el terrestre, marítimo y aéreo, clasificados y conocidos como físicos. En los últimos tiempos, y guiados por la revolución tecnológica, surge la necesidad de explorar y explotar otros dominios tales como; el espacial, ciberespacio y el informacional, también llamado cognitivo.

Al respecto, en el texto, El dominio cognitivo en las operaciones multidominio: concepto y problemática, (Calvo Albero & Garcia Servert, 2022) refieren:

El diseño de un dominio de la información está todavía hoy en una fase incipiente, en la que no hay consenso ni siquiera en su denominación y articulación. EE.UU. habla a veces de entorno (environment) y, a veces, de dominio (domain) de la información, profundamente relacionado con el ciberespacio. La OTAN considera a la información como uno de los entornos o dominios no físicos, en el mismo nivel que el ciberespacio (4º Dominio) y el espacio (5º Dominio), y en España ha tenido éxito la denominación ámbito cognitivo que en líneas generales corresponde a lo que OTAN denomina entorno de la información.

Por su parte, la doctrina conjunta (Estado Mayor Conjunto de las Fuerzas Armadas, 2023) describe, “el instrumento militar debe estar en capacidad de accionar en los diferentes

ámbitos / dominios, aéreo, marítimo, terrestre, espacio, ciberespacio, electromagnético y humano, en una sinergia multiplicadora del poder de combate".

Se puede observar que la información ocupa un espacio de interés dentro de las operaciones militares. La concepción estratégica de capas y restricción de áreas y operaciones multidominio refiere la importancia que recae sobre la información y su gestión. Para lo cual, la inteligencia estratégica, militar y operacional tiene un papel fundamental en alcanzar la eficiencia en el tratamiento de toda información reunida.

El desafío que implica el correcto tratamiento de gran volumen de información requiere de herramientas que faciliten y optimicen su uso. De manera tal facilitar la toma de decisiones, en tiempo, con nivel de certeza razonable.

Por tal motivo, Big Data y la OSINT serán abordadas y analizadas, para conocer cuáles son sus atributos y como pueden emplearse para mejorar la gestión de la información, en el proceso de inteligencia, en apoyo a la toma de decisiones del nivel operacional.

Antecedentes

Es menester destacar que, a la luz de la información considerado elemento sustancial en los conflictos armados, de utilidad esencial en el nivel operacional para el planeamiento y ejecución de las operaciones militares, en un ambiente operacional complejo que requiere integración de gran cantidad de datos e información, se inició la búsqueda del marco conceptual existente.

El ambiente operacional constituye un elemento fundamental en la planificación y ejecución de operaciones militares, define las condiciones físicas, políticas, económicas, sociales y tecnológicas que influyen en el desarrollo de una campaña. (Ejército Argentino, 2015).

Así mismo, se buscó marco teórico que vincule la misma con; el proceso de inteligencia, las herramientas de Big Data y OSINT, contemplando la intención manifiesta en la concepción estratégica de capas y restricción de áreas y operaciones multidominio, descripta en la doctrina del Estado Mayor Conjunto de las Fuerzas Armadas.

Ante ello, podemos destacar el trabajo realizado por el teniente coronel (González Villegas, 2023); propuesta de un modelo conceptual de Big Data para la inteligencia militar, en el cual se propone un modelo conceptual de Big Data que agilice el proceso de información en inteligencia militar considerando el fenómeno de grandes volúmenes de información como resultado del avance de la capacidad de almacenamiento y procesamiento de datos propios del mundo actual.

El discurso del teniente general Guilles Desclaux, en su trabajo Big Data e Inteligencia Artificial para la toma de decisiones militares, trata sobre la importancia que estas herramientas tienen en la toma de decisiones y como cambian el paradigma para llevar a cabo una correcta apreciación de la situación. La integración de Big Data e Inteligencia Artificial en el ámbito militar no solo mejora la eficiencia y efectividad en la toma de decisiones, sino que también plantea importantes retos éticos y de seguridad que deben ser abordados con rigor y responsabilidad. (Desclaux, 2018)

Un aporte claro sobre el tema Big Data es el que se titula: Conociendo el Big Data. El artículo propone, estudiar y analizar de manera exhaustiva el estado del arte del Big Data; además, analizar las características, las herramientas, las tecnologías, los modelos y los estándares relacionados con Big Data e identificar las características más relevantes en la gestión de Big Data. (Camargo Vega, Ortega , & Aguilar , 2014).

Sobre el mismo tema se destaca (Kulshrestha, 2016), en su investigación titulada; Big Data en información e inteligencia militar, analiza las bondades de esta herramienta, comprendiendo los desafíos actuales en materia de toma de decisiones, la cual se ve afectada por su entorno. Concluye que el Big Data tiene un enorme potencial para hacer que las operaciones de las fuerzas armadas sean más eficientes en todo el espectro de su actividad.

Dentro de la temática de inteligencia de fuentes abiertas (OSINT) podemos citar el trabajo de (Las Heras, Diaz Monzón, & Torres, 2016), en él se observa un estudio relacionado a los sesgos tecnológicos, que se ocasiona al igual, o de manera parecida, en el analista de inteligencia. Esta problemática se analiza partiendo del empleo de esta herramienta, se describen sus bondades, pero también, se concluye que es importante controlar los análisis llevados a cabo con estas herramientas.

Otro antecedente de interés es el trabajo llevado a cabo por (Sardá, 2004) quien aborda la gestión de fuentes abiertas y la elaboración de inteligencia útil para la toma de decisiones gubernamentales, en la prevención, anticipación, desactivación de riesgos y amenazas en la seguridad nacional.

Desde el punto de vista de la organización que permite el apoyo de inteligencia al proceso de toma de decisiones de nivel operacional, un aporte a destacar como antecedente es; La organización de la jefatura de inteligencia del comando operacional de las fuerzas armadas en las operaciones multidominio (Arenas, 2021). En este análisis, se puede extraer como valor, la propuesta de considerar los dominios “no físicos”, entendiendo el ciberespacio y el informacional, que configuran un entorno complejo, en consecuencia, la necesidad de establecer un órgano de dirección de inteligencia que permita apoyar la toma de decisiones,

tanto en los ámbitos físicos como los antes mencionados. Además, se analizan las disciplinas de inteligencia que deberían tenerse en cuenta para lograr dicho propósito, aquí se hace presente la inteligencia de fuentes abiertas, y operaciones de información.

También se observa el trabajo de investigación Capacidades, organización e interoperabilidad del Centro Integrador de Inteligencia, en apoyo a una Gran Unidad de Batalla para la toma de decisiones, esgrimiendo las nuevas tecnologías desarrolladas por el Ejército Argentino, en un ambiente operacional complejo – Una propuesta. (Mana, 2018). El mismo busca señalar las modificaciones necesarias en la estructura, organización, equipamiento y las aptitudes que se deben efectuar al Centro Integrador de Inteligencia al implementar nuevas herramientas de conducción desarrolladas por el Ejército Argentino, como ser SITEA y RAIOM, contemplando las características de un ambiente operacional complejo. Aquí, se puede tomar como utilidad la necesidad de rediseñar un Centro Integrador de Inteligencia, como órgano de apoyo a la toma de decisiones, para permitir adaptarse a las nuevas tendencias, herramientas, tecnologías, que implica un ambiente operacional caracterizado por el dinamismo, la rapidez y ambigüedad, y gran cantidad de información.

Estado Actual del Tema

El desarrollo de nuevas tecnologías de la información, en las últimas décadas han crecido vertiginosamente y alcanzados niveles elevados de aplicación en todo el mundo. Sus características disruptivas, implican la necesidad de pensar nuevos paradigmas.

En el marco de los conflictos armados actuales, el uso y proceso de la información es gravitante, elemento esencial para la toma de decisiones, sumado como factor sustancial el tiempo y la integración de datos.

Las tecnologías de la información, sumado a la IA nos brindan herramientas tecnológicas, que pueden aplicarse para contribuir a la gestión de la información en general y en el proceso de inteligencia en particular.

A partir de lo expuesto, el propósito de este trabajo es analizar los atributos de la inteligencia de fuentes abiertas (OSINT) y de Big Data, a fin de valorar su empleo como herramientas que agilicen y mejoren la gestión de la información durante el proceso de inteligencia, en apoyo a la toma de decisiones del nivel operacional en los escenarios actuales.

De los antecedentes revisados se infiere, por tanto, la necesidad de estudiar la trascendencia que adquiere dicha integración de OSINT y Big Data como instrumentos del proceso de inteligencia y como factores que inciden en la oportunidad, pertinencia y calidad de la información disponible para el comandante operacional.

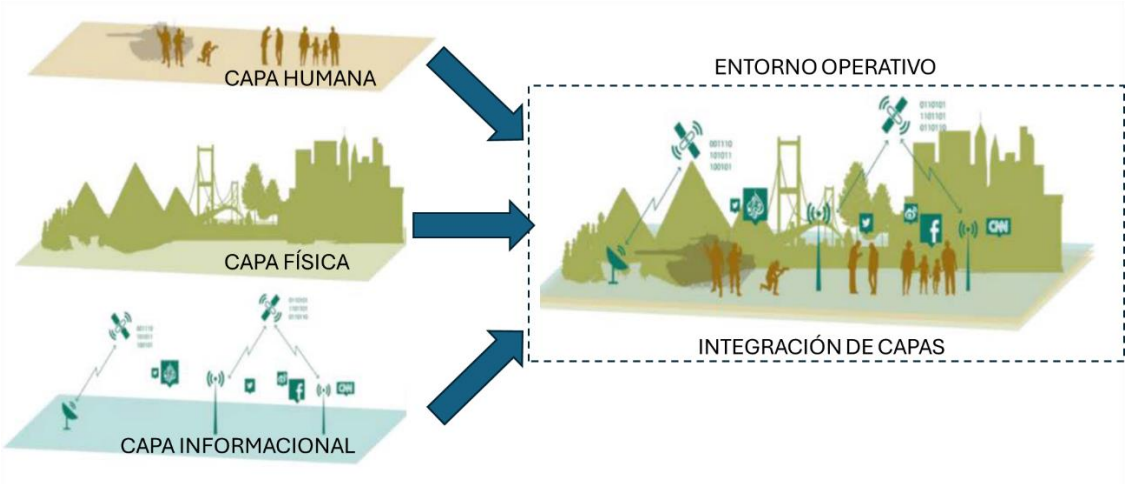
Si bien esta temática fue analizada por diversos autores, en el marco de las operaciones militares y dentro del nivel operacional, no se observa un trabajo integrador efectivo sobre los aspectos antes mencionados.

Por lo antes mencionado y teniendo en cuenta las características de los conflictos actuales, se identifican escenarios en los cuales las fuerzas armadas en su conjunto deberán operar de manera, integrada, con rapidez y capacidad para procesar gran flujo de información permitiendo completar el ciclo de decisión más rápido que el oponente, en un entorno incierto, volátil, ambiguo, complejo, bajo una visión de operaciones multidominio, en ámbitos físicos y no físicos.

La globalización y la hiperconectividad dan lugar a una multitud de factores y actores influyentes que contribuyen al desarrollo de conflictos. El poder se ejerce cada vez más mediante una confluencia de instrumentos híbridos, no se limita a fronteras geográficas. (Smallegange, J. A. P., Bastiaansen, H. J. M., Venema, A. P., & Bronkhorst, A. W, 2018). Estos autores, distinguen tres capas que conforman el entorno operativo. Se considera apropiado exponerlo a continuación para profundizar lo expuesto.

Figura 1

Tres capas del Entorno operativo.



Nota: extraído y modificado de *Big data e inteligencia artificial para la toma de decisiones: Documento de posición holandés*, de Smallegange, J. A. P., Bastiaansen, H. J. M., Venema, A. P., & Bronkhorst, A. W. (2018)

Además, cabe destacar que la integración de OSINT y Big Data en el análisis de inteligencia y la toma de decisiones estratégicas y operacionales ha ganado considerable atención y desarrollo en los últimos años, impulsada por la creciente complejidad de las amenazas y la disponibilidad de tecnologías avanzadas. Se presume que la combinación de

OSINT y Big Data ofrece una sinergia que optimiza la recolección, procesamiento y análisis de datos.

Por su parte cabe recordar que el proceso de inteligencia se compone de diversas fases que incluyen la recolección, procesamiento, análisis y difusión de información. Big Data y OSINT se integran en todas estas fases, permitiendo una recolección de datos más eficiente y un análisis más profundo y preciso. La capacidad de Big Data para proporcionar análisis en tiempo real es crucial para la inteligencia, permitiendo a los analistas identificar amenazas y responder rápidamente a situaciones emergentes.

Aportes Teóricos y/o Prácticos al Campo Disciplinar

Dicho trabajo pretende servir como base investigativa partiendo del análisis, particularmente de dos herramientas, el Big Data y OSINT, considerando sus principales características y atributos en general, que suministren fundamentos para su factibilidad de empleo a fin de optimizar la gestión de información.

Se buscará generar antecedentes sobre su posible empleo, la importancia y efectividad para ser utilizado en el proceso de inteligencia del nivel operacional, que apoya los sistemas de comando y control en la toma de decisiones. Así se observa en el boletín informativo del Estado Mayor Conjunto, cuando habla sobre operaciones multidominio, (Estado Mayor Conjunto de las Fuerzas Armadas, 2023), y refiere: Sistemas de comando y control interconectados en red en condiciones de integrar e interpretar información proveniente de diferentes ámbitos, generando órdenes en cortos espacios de tiempo, haciendo prevalecer el concepto del trienio: inteligencia - velocidad – precisión relativa superior.

Aquí se comprende que es menester plantear la necesidad de considerar el empleo de las herramientas, que favorecen la gestión de la información, siendo hoy un desafío para todos los sistemas de toma de decisiones, y más aún para los decisores militares del nivel operacional.

Objetivos

Objetivo General

Analizar la utilidad de la Inteligencia de Fuentes Abiertas (OSINT) y Big Data para agilizar la gestión de información y mejorar el análisis de inteligencia, con el fin de apoyar de manera efectiva la toma de decisiones en el nivel operacional.

Objetivos Específicos

- Identificar cómo la Inteligencia de Fuentes Abiertas (OSINT) puede mejorar la recolección, procesamiento y análisis de información operacional, y evaluar su impacto en la eficiencia y precisión del proceso de inteligencia.
- Describir la integración de Big Data en el análisis de inteligencia, y determinar cómo esta tecnología puede apoyar la toma de decisiones a nivel operacional, proporcionando datos más profundos y precisos.

Metodología

La presente investigación adopta un enfoque descriptivo y analítico, de carácter fundamentalmente cualitativo, orientado a identificar y examinar las principales características de OSINT y de Big Data, con el propósito de evaluar sus utilidades más relevantes y vincularlas con el proceso de inteligencia y la toma de decisiones en el nivel operacional.

El estudio se inscribe en un diseño no experimental y de tipo documental, basado en el análisis sistemático de fuentes primarias y secundarias. Entre las fuentes primarias se consideran la doctrina conjunta y específica vigente, la normativa asociada, así como libros, artículos académicos y documentos elaborados por autores especializados en inteligencia militar, OSINT y Big Data. Las fuentes secundarias incluyen trabajos de investigación, informes institucionales y publicaciones sobre casos de estudio concretos, cuyo examen permitirá identificar buenas prácticas, limitaciones y lecciones aprendidas.

La técnica principal de recolección y validación de la información será el análisis bibliográfico de carácter lógico y comparativo, que permitirá contrastar los aportes conceptuales de distintos autores y documentos, identificar convergencias y divergencias, y extraer inferencias relevantes para el problema de investigación planteado. Este procedimiento servirá de base para fundamentar, de manera argumentada, las conclusiones acerca de la utilidad de OSINT y Big Data en apoyo a la gestión de la información y a la toma de decisiones en el nivel operacional.

Capítulo I

La inteligencia de fuentes abiertas (OSINT) y la gestión de la información en el proceso de inteligencia operacional

En las operaciones militares contemporáneas, desarrolladas en entornos dinámicos, complejos y fuertemente tecnologizados, la información se ha consolidado como un recurso crítico para la conducción. La doctrina conjunta argentina reconoce que el instrumento militar debe operar de forma integrada en múltiples dominios terrestre, marítimo, aéreo, espacial, ciberespacio, electromagnético y humano, lo que implica enfrentar un volumen y una diversidad de información crecientes que deben ser gestionados por los sistemas de mando, control e inteligencia (Estado Mayor Conjunto de las Fuerzas Armadas, 2018, 2023).

En este contexto, el problema central ya no es la escasez de información, sino la sobreabundancia y la dificultad para identificar, entre grandes volúmenes de datos, aquellos elementos que realmente aportan a la decisión. La inteligencia de fuentes abiertas se presenta, así, como una disciplina que permite aprovechar el enorme caudal de información disponible en medios abiertos, contribuyendo a reducir la incertidumbre y a mejorar la calidad del apoyo al comandante en el nivel operacional (Felip i Sardà, 2004; Las Heras, Díaz Monzón & Blanco Torres, 2017).

Históricamente, la información ha sido un factor clave en los conflictos armados; sin embargo, los avances tecnológicos de las últimas décadas han modificado cualitativamente su rol. El desarrollo de internet, la masificación de dispositivos móviles y la expansión de redes de sensores han generado un entorno en el que se producen, almacenan y transmiten datos en volúmenes sin precedentes (Camargo Vega, Camargo Ortega & Joyanes Aguilar, 2014).

Esta transformación impacta directamente en la conducción de las operaciones. La posibilidad de contar con información más completa, actualizada y precisa puede otorgar ventajas decisivas, siempre que el sistema de inteligencia sea capaz de procesarla y analizarla en tiempos compatibles con el ciclo de decisión operacional. De lo contrario, la abundancia de datos puede devenir en saturación y, paradójicamente, en parálisis del proceso decisorio (Las Heras et al., 2017).

Treverton (2001) sostiene que, en la "era de la información", los servicios de inteligencia ya no operan solamente en el tradicional "negocio de los secretos", sino en el "negocio de la información", caracterizado por múltiples objetivos, numerosos consumidores y un exceso de datos de calidad dispar. En ese contexto, las fuentes abiertas pasan a ser un insumo central, pero al mismo tiempo amplifican el problema de la sobreabundancia

informativa, obligando a desarrollar capacidades analíticas y tecnológicas que permitan discriminar qué datos son realmente relevantes para la acción estatal.

En este marco, la OSINT y las capacidades asociadas a Big Data, analizadas en detalle en el capítulo II, constituyen herramientas fundamentales para gestionar de manera más eficiente la información que alimenta la inteligencia militar, en coherencia con la orientación de la doctrina conjunta hacia las operaciones conjuntas y multidominio (Estado Mayor Conjunto de las Fuerzas Armadas, 2018, 2023).

Conceptualización de OSINT y evolución de las fuentes abiertas

OSINT ha pasado, en pocas décadas, de ocupar un lugar marginal en los servicios de inteligencia a ser considerada una disciplina imprescindible para comprender entornos complejos, caracterizados por la abundancia de información y la convergencia de amenazas.

En términos generales, puede definirse OSINT como el proceso sistemático de búsqueda, selección, recopilación, procesamiento y análisis de información procedente de fuentes accesibles al público, orientado a producir conocimiento útil para la toma de decisiones de gobiernos, fuerzas armadas u otras organizaciones (Felip i Sardà, 2004; Lowenthal, 2012; Las Heras, Díaz Monzón & Blanco Torres, 2017).

Lowenthal y Clark describen la OSINT como el uso de información disponible públicamente y su análisis para informar procesos de decisión, subrayando que lo decisivo no es el carácter "abierto" de los datos, sino el tratamiento analítico que los convierte en inteligencia (Lowenthal, 2012).

En la misma línea, diversos manuales doctrinarios definen OSINT como inteligencia obtenida a partir de información deliberadamente descubierta, depurada y difundida desde fuentes abiertas, de acuerdo con necesidades específicas de información (NATO, 2001; EMCO, 2018).

Desde esta perspectiva, no toda información abierta es automáticamente OSINT: el rasgo distintivo es la aplicación del método de inteligencia (dirección–obtención–procesamiento–análisis–difusión) a datos accesibles al público, generando productos adaptados a los requerimientos de un decisor concreto (Williams, 2018).

Felip i Sardà (2004) destaca que la gestión de fuentes abiertas se ha vuelto esencial para la elaboración de la inteligencia necesaria en la prevención, anticipación y desactivación de riesgos y amenazas.

Según este autor, a medida que la seguridad adquiere una dimensión más amplia, incluyendo aspectos políticos, económicos, sociales, tecnológicos y medioambientales, el

abanico de fuentes potencialmente relevantes crece de forma exponencial, y una parte significativa de esa información se encuentra abierta para su uso.

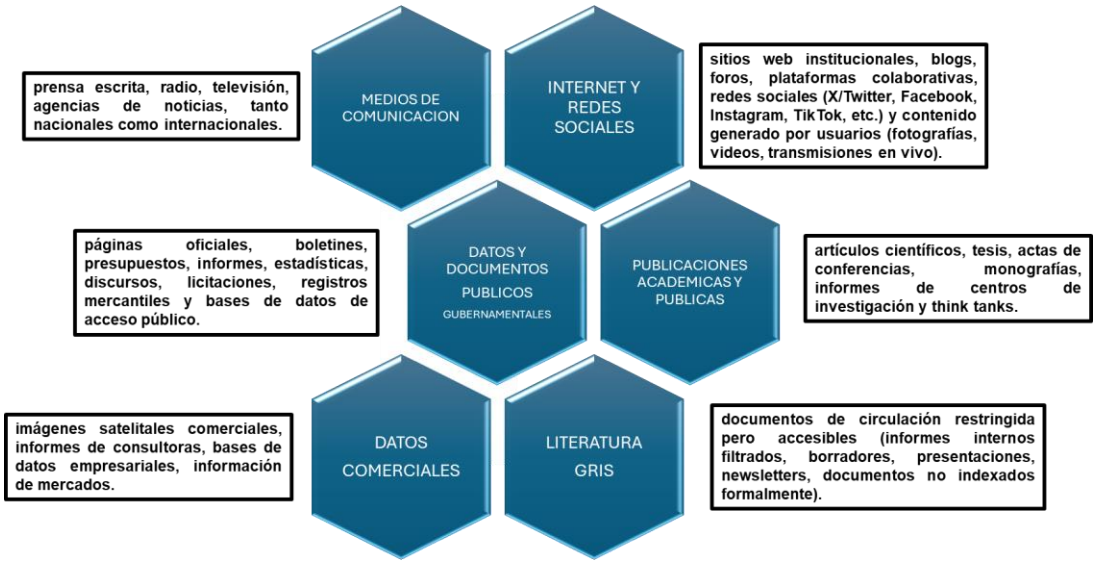
Por su parte, Las Heras et al. (2017) insisten en que OSINT no debe confundirse con una mera actividad de "búsqueda en internet". Se trata de una disciplina de inteligencia que exige reglas de obtención, criterios de evaluación de fuentes, procedimientos de contraste y estándares de validación, especialmente cuando se utilizan herramientas tecnológicas que pueden introducir sesgos en el análisis.

En el ámbito militar, autores como Ziółkowska (2018) sostienen que OSINT constituye hoy un componente legítimo y eficaz del reconocimiento militar, complementando a otras disciplinas como HUMINT, SIGINT o IMINT, y aportando contexto político, social y mediático para comprender mejor la situación operacional.

La expansión de OSINT está directamente vinculada a la multiplicación de tipos de fuentes abiertas disponibles. En la literatura se suelen distinguir, entre otras, las siguientes categorías (Felip i Sardà, 2004; NATO, 2001)

Figura 2

Tipos de fuentes abiertas.



Fuente: elaboración propia.

Como señalan varias aproximaciones recientes, el núcleo de OSINT en la práctica actual se encuentra en la intersección entre estos tipos de fuentes, especialmente en el cruce entre medios tradicionales, redes sociales, bases de datos públicas y productos comerciales (Williams, 2018; Van Puyvelde, 2022).

La evolución histórica de OSINT también ha sido objeto de análisis. Algunos trabajos especialmente en el ámbito de Estados Unidos y la OTAN, distinguen entre una "primera

generación" de OSINT, centrada en la explotación de medios tradicionales y documentos públicos, y una "segunda generación", vinculada al auge de internet, las redes sociales y el Big Data (Hulnick, 2010; Williams, 2018).

En la primera generación, el foco estaba en la traducción y análisis de prensa extranjera, emisiones de radio y televisión, publicaciones oficiales y literatura académica.

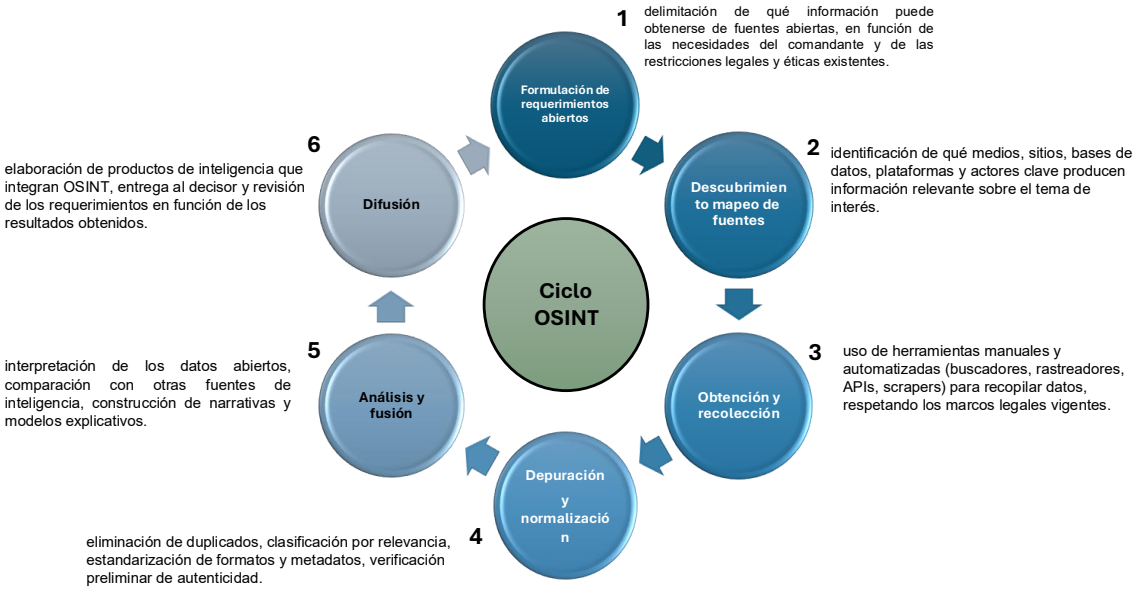
En la segunda generación, la atención se desplaza hacia entornos digitales, donde el volumen, la velocidad y la variedad de la información se multiplican, y donde actores estatales y no estatales compiten activamente por el control de narrativas y percepciones.

Van Puyvelde (2022) advierte, sin embargo, que la idea de OSINT como una "revolución" exclusivamente derivada de la explosión de datos abiertos resulta engañosa. Más bien, se trata de una continuidad con cambios graduales, donde la digitalización intensifica y acelera procesos ya existentes, pero no altera la lógica básica de la inteligencia de fuentes abiertas.

Si bien OSINT se integra en el ciclo general de inteligencia, numerosos autores destacan la existencia de un ciclo OSINT específico, con características propias (NATO, 2001; Williams, 2018):

Figura 3

Ciclo OSINT



Fuente: elaboración propia.

Este ciclo pone de relieve que el valor de la OSINT no reside solo en "encontrar" información, sino en integrarla de manera coherente y crítica en el proceso de inteligencia

multifuente, evitando tanto la duplicación de esfuerzos como la dependencia exclusiva de las fuentes abiertas.

Información, dominio cognitivo, operaciones multidominio y OSINT.

En la doctrina contemporánea, la información ha dejado de concebirse exclusivamente como un insumo para el proceso de inteligencia y se reconoce, además, como un dominio estrechamente vinculado al ámbito cognitivo (Calvo Albero & García Servert, 2021). Esta perspectiva resulta coherente con el enfoque de las operaciones multidominio, que entiende que la disputa por la superioridad informacional y la influencia sobre percepciones, narrativas y voluntades puede ser tan decisiva como la que se libra en los dominios físico y no físico (EMCO, 2023). En consecuencia, el espacio informacional - cognitivo se configura como un ámbito donde se planifican, conducen y evalúan operaciones con efectos concretos sobre el comportamiento de actores estatales y no estatales.

Esta revalorización de la información se articula con el enfoque de operaciones multidominio, que reconoce que los efectos generados en los dominios terrestre, marítimo, aéreo, ciber y espacial convergen, en última instancia, en el ámbito cognitivo: la mente de los decisores, las tropas y las audiencias relevantes. En este marco, la disputa por la superioridad informacional - entendida como la capacidad de adquirir, procesar, proteger y explotar la información más rápido y mejor que el adversario - puede ser tan decisiva como la que se libra en los dominios físico y ciber (EMCO, 2023). Así, el espacio informacional - cognitivo se configura como el punto de encuentro donde las acciones en cada dominio buscan producir efectos coordinados sobre la percepción y la voluntad del oponente.

Dentro de este entramado, la inteligencia de fuentes abiertas (OSINT) se ubica en la intersección entre la función clásica de apoyo a la decisión y la lógica de las operaciones en el dominio informacional. Su valor no se limita a “alimentar” al ciclo de inteligencia, sino a contribuir directamente a la generación de ventajas en el plano cognitivo, al identificar y explotar oportunidades y vulnerabilidades informacionales del adversario.

Esta concepción se apoya en la doctrina de la OTAN sobre OSINT como componente esencial de las operaciones de información (NATO, 2001).

En este contexto, siguiendo la tipología de productos de inteligencia propuesta por Pherson & Pherson (2016) y Moore (2005), puede sostenerse que la OSINT cumple funciones descriptivas, explicativas y proyectivas, esta última en el sentido de análisis estimativo o prospectivo, a saber:

Función descriptiva: ofrece una imagen más completa y matizada de la situación a partir de la integración de múltiples fuentes abiertas (medios de comunicación, redes sociales, bases de datos académicas, informes de organismos internacionales, entre otros). Ello permite reducir incertidumbres iniciales y complementar la información proveniente de fuentes clasificadas.

Función explicativa: contribuye a comprender motivaciones, percepciones, marcos narrativos y líneas de argumentación de actores estatales y no estatales. El análisis sistemático del discurso público, de las campañas de comunicación y de la interacción en plataformas digitales permite identificar los relatos que buscan legitimar decisiones, movilizar apoyos o deslegitimar al adversario.

Función proyectiva: facilita la identificación de tendencias, riesgos emergentes y posibles cursos de acción del adversario, especialmente en el plano informacional y cognitivo. El monitoreo continuo de señales débiles y patrones de comportamiento en el espacio informativo puede anticipar campañas de desinformación, operaciones psicológicas o intentos de influencia sobre audiencias clave.

De este modo, la OSINT se convierte en un componente esencial para la construcción de una conciencia situacional ampliada, que contemple no sólo las capacidades materiales del adversario, sino también su dimensión simbólica, comunicacional y cognitiva (Calvo Albero & García Servert, 2021).

Integrada en un enfoque de operaciones multidominio, la explotación sistemática de fuentes abiertas contribuye a articular mejor los efectos deseados en todos los niveles, actuando en las capas física, humana e informacional.

Aportes de la OSINT a cada fase del proceso de inteligencia

En el apartado precedente se ha argumentado que la información constituye, en la doctrina contemporánea, un dominio estrechamente vinculado al ámbito cognitivo y a la lógica de las operaciones multidominio. En ese marco, la inteligencia de fuentes abiertas (OSINT) se configura como un recurso crítico para la generación de superioridad informacional, en tanto posibilita la observación sistemática del entorno, el seguimiento de narrativas y la identificación de tendencias que inciden sobre la percepción y la voluntad de los actores.

Sobre esta base conceptual, resulta pertinente examinar de qué manera el potencial de la OSINT se operacionaliza a lo largo del ciclo de inteligencia. Más allá de su carácter transversal, interesa aquí identificar sus contribuciones específicas en cada fase (dirección y planeamiento, obtención, procesamiento, análisis y producción, y difusión), atendiendo tanto a las oportunidades que ofrece para mejorar la oportunidad, pertinencia y calidad del apoyo al

comando, como a las limitaciones y desafíos que plantea su integración con las restantes disciplinas de inteligencia.

Dirección

En la fase de dirección, la OSINT contribuye a delimitar las Necesidades Esenciales de Información (NEI)[1] del comandante, al brindar un panorama preliminar de actores, escenarios y dinámicas relevantes en el área de operaciones. Esta visión inicial, apoyada en fuentes abiertas y herramientas de análisis de grandes volúmenes de datos, facilita la formulación de requerimientos más precisos y focalizados, evitando esfuerzos de obtención dispersos o redundantes (Arenas, 2021). De este modo, la OSINT se integra tempranamente en el ciclo de inteligencia, orientando de forma más eficiente la asignación de medios y prioridades de búsqueda.

Obtención

En la fase de obtención, la OSINT amplía significativamente el espectro de fuentes disponibles: medios tradicionales, portales digitales, redes sociales, sitios oficiales, bases de datos públicas, repositorios académicos e imágenes satelitales comerciales, entre otros. Felip i Sardà (2004) enfatiza que, en muchos contextos, las fuentes abiertas ofrecen información rápida, de bajo costo y de gran valor contextual, especialmente cuando las posibilidades de obtención sobre el terreno son limitadas o riesgosas. El empleo de buscadores avanzados, herramientas de monitoreo automatizado y sistemas de explotación de Big Data permite, además, captar señales débiles y variaciones en el entorno que podrían pasar inadvertidas mediante métodos tradicionales.

Procesamiento

El procesamiento de OSINT implica tareas de depuración, clasificación, estructuración y verificación de la información recolectada. Las Heras et al. (2017) alertan sobre los sesgos tecnológicos que pueden introducirse cuando se utilizan herramientas automatizadas de recolección y análisis, lo que exige una evaluación crítica de los algoritmos, plataformas y criterios de filtrado empleados. En el nivel operacional, donde el tiempo es un recurso escaso, un procesamiento eficiente de OSINT resulta decisivo para evitar la saturación de los analistas y garantizar que la información relevante llegue al decisor sin demoras innecesarias. La incorporación de técnicas de minería de datos, análisis de redes y visualización contribuye a transformar grandes volúmenes de datos abiertos en insumos inteligibles y priorizados.

[1] NEI: Utilizada como sinónimo de Elementos Esenciales de Inteligencia (EEI). A fin de englobar la conceptualización de varios autores orientados al análisis de OSINT.

Análisis

Durante el análisis, la OSINT se integra con otras disciplinas de inteligencia para construir productos multifuente. En esta etapa, la información abierta aporta contexto político, económico y social; permite seguir la evolución de narrativas y percepciones; y contribuye a identificar patrones de comportamiento y redes de relaciones entre actores (Las Heras et al., 2017).

El desafío consiste en combinar la riqueza y amplitud de la OSINT con la profundidad que proporcionan fuentes más sensibles, evitando la dependencia exclusiva de una sola disciplina y reduciendo la probabilidad de errores analíticos (Mana, 2018; Lowenthal, 2012). En este sentido, los datos abiertos pueden validar o matizar hipótesis formuladas a partir de fuentes clasificadas, así como ofrecer indicadores adicionales para la elaboración de escenarios prospectivos y estimaciones de riesgo.

Difusión

En la fase de difusión, la integración adecuada de OSINT en los productos de inteligencia permite ofrecer al comandante informes más completos y visualmente claros (mapas, cronologías, tableros, matrices de actores, redes de vínculos), lo que facilita la comprensión y el uso de la información en el planeamiento y la conducción de operaciones (EMCO, 2018; Arenas, 2021). La posibilidad de representar gráficamente datos extraídos de fuentes abiertas, por ejemplo, actividad en redes sociales, variaciones en indicadores socioeconómicos o cambios en la presencia de actores en el terreno, refuerza la capacidad del decisor para valorar alternativas de acción y ajustar en tiempo casi real sus cursos de acción.

En conjunto, la OSINT recorre todo el ciclo de inteligencia, desde la definición de necesidades hasta la difusión de productos, agregando valor añadido en cada fase e incrementando la oportunidad, pertinencia y calidad del apoyo a la decisión.

Conclusiones parciales

Dado lo expresado, relativo al papel de la información y de la OSINT en el proceso de inteligencia operacional, se puede inferir que;

La información se ha consolidado como un recurso crítico y como un dominio de disputa estrechamente vinculado al ámbito cognitivo.

El problema central ya no es la escasez de datos, sino la sobreabundancia, lo que exige desarrollar capacidades específicas para seleccionar, procesar y emplear oportunamente aquella información que agrega valor al planeamiento y a la conducción de las operaciones.

La OSINT se configura como una disciplina de inteligencia que aplica de manera sistemática y técnica, el método de inteligencia a datos accesibles al público, lo que permite diferenciarla claramente de la simple búsqueda de información en internet.

Su evolución, de una primera etapa, centrada en medios tradicionales, hacia una segunda, marcada por entornos digitales, redes sociales y Big Data, amplía su alcance, su velocidad y la complejidad de su gestión.

La OSINT contribuye a la generación de superioridad informacional mediante funciones descriptivas, explicativas y proyectivas, que inciden directamente en el ámbito cognitivo de decisores, tropas y audiencias, enriqueciendo la conciencia situacional.

El ciclo de inteligencia aporta el marco metodológico indispensable para que la OSINT genere verdadero valor en el nivel operacional, convierte el volumen disperso de datos abiertos en productos de inteligencia pertinentes, oportunos, reduciendo la incertidumbre del comandante y contribuyendo de forma concreta a la superioridad informacional en las operaciones.

Capítulo 2

Integración de Big Data en el análisis de inteligencia y su impacto en la toma de decisiones operacionales

Mientras que en el capítulo anterior se analizó el papel de la inteligencia de fuentes abiertas (OSINT) en la gestión de la información, aquí se aborda la dimensión tecnológica y analítica que introduce Big Data en el proceso de inteligencia. El foco se sitúa en cómo el tratamiento masivo de datos - estructurados y no estructurados - potencia la producción de inteligencia militar en entornos de operaciones conjuntas y multidominio, caracterizados por la abundancia de información, la conectividad permanente y la aceleración de los ciclos de decisión (EMCO, 2018, 2023). En este contexto, el desafío ya no radica únicamente en acceder a la información, sino en ser capaces de procesarla, integrarla y explotarla antes que el adversario.

Big Data se presenta, en consecuencia, como una capacidad habilitante que permite transformar el tradicional enfoque de análisis sobre conjuntos de datos acotados hacia un modelo orientado al volumen, la variedad y la velocidad de los flujos de información, incorporando además consideraciones de veracidad y valor para la decisión.

Tal como señalan Gandomi y Haider (2015), el aporte central de Big Data no reside solo en la magnitud de los datos disponibles, sino en la posibilidad de aplicar técnicas analíticas avanzadas, como ser; minería de datos, aprendizaje automático, análisis predictivo, para extraer patrones, tendencias y relaciones que serían difíciles de detectar mediante métodos convencionales.

Desde la perspectiva operacional, este giro analítico adquiere relevancia particular. La integración de fuentes provenientes de sensores, sistemas ISR, registros de plataformas, comunicaciones, ciberespacio y, de manera creciente, de entornos civiles (tráfico, redes sociales, datos comerciales, entre otros) puede contribuir a mejorar la conciencia situacional, anticipar amenazas, optimizar el empleo de recursos y respaldar al comandante operacional con productos de inteligencia de mayor calidad (Haridas, 2015).

No obstante, ello exige repensar arquitecturas, procedimientos y competencias del personal de inteligencia, de modo que la incorporación de Big Data no se limite a una actualización tecnológica, sino que se integre coherentemente en el ciclo de inteligencia y en la planificación de las operaciones.

Definiciones de Big Data y características principales

El concepto de Big Data ha sido definido de múltiples formas en la literatura especializada. Un enfoque ampliamente aceptado lo describe a partir del modelo de las llamadas "V" de los datos: volumen, referido a la enorme cantidad de información disponible; velocidad, asociada a la rapidez con la que se generan, transmiten y procesan esos datos; y variedad, vinculada a la heterogeneidad de formatos y fuentes.

Sobre esta base, con el tiempo se han incorporado otras dimensiones, como la veracidad, esto es, la calidad, fiabilidad y consistencia de los datos y el valor, entendido como la capacidad de transformar dichos datos en conocimiento útil para la toma de decisiones (Camargo Vega et al., 2014; Gandomi & Haider, 2015).

Gandomi y Haider (2015) destacan que Big Data no se reduce al tamaño de los conjuntos de datos, sino que implica la adopción de nuevas formas de captura, almacenamiento y análisis, especialmente de datos no estructurados (texto, imágenes, audio, video) que constituyen hoy la mayor parte de la información disponible.

En esta línea, Big Data puede definirse como un conjunto integrado de tecnologías, arquitecturas y metodologías que permite gestionar grandes volúmenes de datos heterogéneos, generados a alta velocidad, con el propósito de transformarlos en conocimiento accionable para distintos niveles decisorios.

Desde la perspectiva de autores, como Camargo Vega et al. (2014), el fenómeno Big Data surge de la convergencia entre el crecimiento exponencial de los datos, el desarrollo de capacidades de procesamiento distribuido y la maduración de técnicas de analítica avanzada. Esta confluencia abre nuevas posibilidades para organizaciones públicas y privadas, entre ellas, las instituciones de seguridad y defensa, al facilitar un análisis más profundo y oportuno de la información relevante para la planificación, la conducción y la evaluación de acciones en entornos complejos.

Las "V" del Big Data y su aporte a la toma de decisiones operacionales

La caracterización de Big Data a través de las "V" permite comprender mejor su aporte concreto al proceso de toma de decisiones, en particular en el nivel operacional. Cada una de estas dimensiones se vincula con capacidades específicas para la producción de inteligencia y la reducción de la incertidumbre en entornos complejos (Camargo Vega et al., 2014; Gandomi & Haider, 2015).

Volumen: alude a la enorme cantidad de datos disponibles, provenientes de múltiples sensores, sistemas de información, redes sociales y fuentes abiertas. En el nivel operacional, este volumen permite construir una imagen más completa del ambiente operacional, siempre

que exista capacidad para filtrar y priorizar la información relevante. (Camargo Vega et al., 2014; Mayer-Schönberger & Cukier, 2013).

Velocidad: refiere a la rapidez con la que se generan, transmiten y procesan los datos. En contextos de operaciones conjuntas y multidominio, la velocidad es crítica para acortar los ciclos de decisión del comandante y permitir respuestas oportunas frente a cambios en la situación. (EMCO, 2018, 2023; Gandomi & Haider, 2015).

Variedad: expresa la diversidad de formatos (texto, imágenes, video, señales, registros transaccionales, entre otros) y de fuentes (abiertas, comerciales, institucionales). Esta variedad enriquece la inteligencia al ofrecer múltiples perspectivas sobre un mismo fenómeno, pero exige metodologías robustas de integración y correlación de datos. (Gandomi & Haider, 2015; Weng & Wu, 2024).

Veracidad: se vincula con la calidad, confiabilidad y consistencia de los datos. En el ámbito operacional, la veracidad resulta central para reducir la incertidumbre, evitar sesgos en el análisis y disminuir el riesgo de decisiones basadas en información engañosa o manipulada. (Camargo Vega et al., 2014; Mayer-Schönberger & Cukier, 2013).

Valor: hace referencia a la capacidad de transformar datos en conocimiento útil para la acción. No todo dato disponible se traduce automáticamente en valor operativo; este surge cuando los datos son tratados mediante técnicas analíticas adecuadas y se integran en productos de inteligencia que apoyan decisiones concretas de planificación, conducción y evaluación de operaciones. (Gandomi & Haider, 2015; Marr, 2016).

Tipos de datos relevantes para la inteligencia militar

En el ámbito militar, Big Data se caracteriza no solo por el volumen de información disponible, sino, sobre todo, por su variedad: conviven datos estructurados, semiestructurados y no estructurados que se generan a gran velocidad y desde múltiples fuentes (sensores, sistemas de armas, redes de comunicaciones, plataformas abiertas, etc.).

Esta diversidad plantea desafíos específicos de integración y análisis, pero también abre la posibilidad de construir una imagen mucho más rica del entorno operacional (Gandomi & Haider, 2015).

La literatura especializada en Big Data subraya que, en términos cuantitativos, la mayor parte de los datos disponibles es no estructurada (texto, audio, imagen, video), lo que obliga a combinar técnicas clásicas de análisis con herramientas avanzadas como minería de datos, aprendizaje automático y analítica visual interactiva (Gandomi & Haider, 2015).

En defensa y seguridad, esto se traduce en la necesidad de articular, dentro de un mismo entorno analítico, datos procedentes de sensores militares, sistemas administrativos y fuentes abiertas, alineando la lógica del ciclo de inteligencia con las capacidades de Big Data (Haridas, 2015; Lim, 2016).

Datos estructurados

Los datos estructurados son aquellos organizados en tablas o esquemas relacionales, con campos y registros bien definidos. En el contexto militar, incluyen, entre otros:

- Registros de sensores integrados en sistemas de armas (por ejemplo, parámetros de tiro, telemetría de misiles, registros de mantenimiento).
- Bases de datos logísticas: existencias de munición, repuestos, combustible, tiempos de entrega, contratos de apoyo.
- Posiciones y movimientos de unidades registradas en sistemas de comando y control (C2/C4ISR).
- Historiales de vuelo y de navegación, planes de misión.
- Datos administrativos de personal (dotaciones, rotaciones, calificaciones, horas de adiestramiento).

Este tipo de datos es especialmente relevante para construir indicadores y modelos predictivos sobre disponibilidad de medios, niveles de alistamiento, consumo logístico, desgaste de plataformas o patrones de despliegue.

Estudios sobre Big Data en defensa muestran que la explotación sistemática de estos registros permite, por ejemplo, mejorar la planificación de mantenimiento, optimizar el empleo de flotas de UAV y reducir tiempos de respuesta ante incidentes.

En términos de proceso de inteligencia, los datos estructurados tienden a ser la base de productos cuantitativos (estadísticas, series temporales, modelos de riesgo) que apoyan al nivel operacional y estratégico en el diseño de cursos de acción, análisis de tendencias y evaluación de resultados de operaciones (Lim, 2016).

Datos semiestructurados

Los datos semiestructurados presentan un cierto grado de organización interna (etiquetas, metadatos, campos predefinidos), pero no se ajustan completamente a las restricciones de las bases relacionales. En el ámbito militar, pueden mencionarse:

- Registros (logs) de sistemas de mando y control, redes y servidores.
- Metadatos de comunicaciones (fechas, horarios, remitentes/destinatarios, geolocalización aproximada, tipo de dispositivo).

- Mensajes operacionales con formatos estandarizados (plantillas de informes, partes de situación).
- Alertas y eventos generados de manera automatizada por sistemas de vigilancia, ciberdefensa o sensores distribuidos en un teatro de operaciones.

En los sistemas de comando y control en el ciberespacio, estos datos semiestructurados son críticos para detectar patrones anómalos, correlacionar eventos y producir alertas tempranas sobre intrusiones, ataques distribuidos o degradación de servicios esenciales (Haji Molla Mirzaie et al., 2021).

Desde la perspectiva del ciclo de inteligencia, los datos semiestructurados funcionan como un puente entre lo estrictamente cuantitativo (bases de datos) y lo cualitativo (informes narrativos), pues conservan suficiente estructura para la automatización, pero a la vez capturan la dinámica y secuencia de los eventos operativos (Gandomi & Haider, 2015).

Datos no estructurados

Los datos no estructurados abarcan la información que no se ajusta a un formato predefinido y que, por ello, requiere técnicas avanzadas de procesamiento:

- Texto libre: informes de inteligencia, actas de reunión, partes de combate, transcripciones de interrogatorios, documentos doctrinarios.
- Contenidos mediáticos y de redes sociales: noticias, publicaciones en plataformas sociales, blogs, foros, mensajería instantánea.
- Imágenes: productos de satélites, UAV, sensores optrónicos, cámaras tácticas o sistemas de vigilancia fija.
- Audio: emisiones radiales, comunicaciones interceptadas, grabaciones de canales de mando y control.
- Video: flujos de UAV armados y no armados, sistemas de vigilancia terrestre, cámaras corporales o embarcadas.

En el campo de la vigilancia y el reconocimiento, Bognár (2020) muestra que la mayor parte de los datos generados por sistemas de vigilancia militar proviene de sensores que producen imágenes y video, junto con OSINT, y que el desafío central ya no es obtener información, sino extraer valor de esa masa de datos en tiempo oportuno.

Desde una perspectiva más general, Gandomi y Haider (2015) destacan que los datos no estructurados —texto, audio, imagen, video— representan la mayoría de los volúmenes de Big Data, y que precisamente ahí se concentran muchos de los aportes más innovadores de la

analítica (minería de texto, reconocimiento automático de imágenes, análisis de sentimiento, etc.).

En inteligencia militar, esto se traduce en capacidades como:

- Detección de cambios en imágenes satelitales o de UAV (movimientos de unidades, construcción de infraestructuras, actividad en aeródromos o puertos).
- Identificación automática de personas, emblemas o vehículos en secuencias de video.
- Análisis de narrativas y percepciones en redes sociales en torno a operaciones, crisis o acciones de fuerzas propias y adversarias.
- Búsqueda de patrones lingüísticos y semánticos en grandes volúmenes de texto para apoyar el análisis de amenazas terroristas, criminales o híbridas (Lim, 2016)

Diversos estudios coinciden en que el verdadero salto cualitativo no reside en tratar cada tipo de dato por separado, sino en integrarlos en un entorno analítico común, capaz de combinar datos estructurados, semiestructurados y no estructurados en apoyo al ciclo de inteligencia y de la toma de decisiones (Haridas, 2015; Bognár, 2020).

Big Data en el ciclo de inteligencia

La integración de Big Data no altera la estructura básica del ciclo de inteligencia, pero sí transforma la forma en que se ejecutan sus fases (EMCO, 2018).

Dirección

El acceso a grandes volúmenes de datos históricos y en tiempo real permite formular requerimientos de inteligencia más complejos, relacionados con patrones de comportamiento, detección de anomalías o correlaciones entre eventos en dominios diversos. El comandante y su Estado Mayor pueden plantear preguntas que exceden el alcance de métodos tradicionales de análisis, apoyándose en capacidades analíticas automatizadas (González Villegas, 2024; Haridas, 2015).

Obtención

La obtención deja de centrarse exclusivamente en informes discretos y se amplía a flujos continuos de datos (streams) provenientes de sensores ISR, sistemas de mando y control, plataformas digitales y fuentes abiertas. Big Data posibilita la ingesta simultánea de múltiples fuentes de información en tiempo casi real (Kulshrestha, 2016).

Procesamiento

Infraestructuras de almacenamiento distribuido y procesamiento paralelo, por ejemplo, clústeres de cómputo o soluciones en nube privada, permiten depurar, organizar y fusionar

volúmenes masivos de datos en plazos compatibles con el ciclo de decisión operacional. Este procesamiento incluye tareas de limpieza, normalización, correlación y enriquecimiento de datos (Camargo Vega et al., 2014).

Análisis

Técnicas de minería de datos, aprendizaje automático y análisis de redes facilitan la identificación de patrones, tendencias y nodos críticos que serían difíciles de detectar con métodos puramente manuales. Gandomi y Haider (2015) resaltan que la clave reside en seleccionar adecuadamente los métodos analíticos según el problema a resolver, evitando un uso indiscriminado de algoritmos que pueda generar resultados poco fiables.

Difusión

Herramientas de visualización (tableros de mando, mapas dinámicos, indicadores clave) permiten entregar al decisor información sintética, priorizada y actualizada. De este modo, los productos de inteligencia se presentan de forma más intuitiva, facilitando su incorporación en el planeamiento y la conducción de operaciones (González Villegas, 2024).

Big Data reconfigura el ciclo de inteligencia como un proceso intensivo en datos y analítica, donde la generación de conocimiento depende tanto de la calidad de la información de entrada como de la adecuación de las herramientas analíticas empleadas (Haridas, 2015).

Big Data, operaciones multidominio y concepción estratégica de capas

La doctrina argentina sobre operaciones multidominio y concepción estratégica de capas plantea que el instrumento militar debe coordinar acciones en dominios físicos (terrestre, marítimo, aéreo, espacial) y no físicos (informacional, cognitivo, ciberespacio), con el propósito de obtener ventajas combinadas y explotar las interdependencias entre dichos dominios (EMCO, 2023).

En este marco, Big Data cumple un rol central, ya que permite:

- Correlacionar datos de múltiples dominios, por ejemplo, patrones de actividad en redes sociales, movimientos logísticos, indicadores económicos y ciber incidentes.
- Analizar las interacciones entre capas de la concepción estratégica —territorial, informática, cognitiva—, identificando cómo acciones en un ámbito (por ejemplo, el informacional) pueden producir efectos en el terreno o en la voluntad de combate.
- Construir una imagen operacional común más rica, en la que se integren datos geoespaciales, información de inteligencia, variables socioeconómicas y registros

logísticos en una misma representación (Calvo Albero & García Servert, 2021; EMCO, 2023).

King (2024) analiza cómo las fuerzas armadas de la OTAN buscan "aprovechar el poder del Big Data, analizado a velocidad y escala mediante algoritmos", para mejorar la comprensión del campo de batalla y, especialmente, los procesos de targeting. El autor muestra que la inteligencia artificial se ha empleado, ante todo, para procesar grandes volúmenes de datos, satélites, SIGINT, HUMINT y OSINT, acelerando los ciclos de inteligencia y mejorando la precisión en la selección de objetivos, más que para automatizar por completo el empleo de la fuerza (King, 2024).

Así, Big Data se transforma en una herramienta clave para materializar la concepción por capas, al proporcionar los medios para capturar, integrar y analizar información procedente de los distintos ámbitos de interés operacional y apoyar procesos como el targeting en un entorno multidominio.

Impacto de Big Data en la toma de decisiones en el nivel operacional

En el nivel operacional, el comandante debe planear y conducir campañas que articulan múltiples operaciones tácticas, bajo una lógica coherente con los objetivos estratégicos. La integración de Big Data en el sistema de inteligencia puede apoyar esta tarea en, al menos, tres planos de analítica:

Analítica descriptiva – "¿Qué está ocurriendo?"

Tableros de situación que integran datos de sensores, sistemas de mando y control, registros logísticos y fuentes abiertas, ofreciendo una visión unificada del ambiente operacional.

Mapas dinámicos que muestran la disposición de fuerzas propias y adversarias, la configuración del terreno, los flujos de población y otros factores clave (González Villegas, 2024).

Analítica predictiva – "¿Qué podría ocurrir?"

Modelos que estiman probabilidades de determinados cursos de acción del adversario, basados en datos históricos y en señales observadas en tiempo real.

Análisis de tendencias logísticas y operacionales que permiten anticipar cuellos de botella en abastecimientos, mantenimiento o rotación de fuerzas (Kulshrestha, 2016; Haridas, 2015).

Analítica prescriptiva – "¿Qué conviene hacer?"

Herramientas de optimización que ayudan a asignar recursos entre distintas áreas u operaciones, en función de restricciones de tiempo, espacio y medios disponibles.

Simulaciones y análisis de escenarios que permiten comparar cursos de acción y evaluar sus riesgos y ventajas en términos de eficacia, eficiencia y efectos esperados (Desclaux, 2018; González Villegas, 2024).

Estas capacidades no sustituyen el juicio profesional del comandante, pero proporcionan un soporte cuantitativo y cualitativo que puede mejorar significativamente la calidad de las decisiones, en particular cuando se trata de manejar grandes volúmenes de información y múltiples variables simultáneas.

Desafíos y riesgos de la integración de Big Data con el análisis de inteligencia.

La incorporación de Big Data en la inteligencia militar no es neutra ni exenta de tensiones. Supone reconfigurar procesos, estructuras y culturas organizacionales, al tiempo que introduce nuevas dependencias tecnológicas, dilemas éticos y riesgos operativos que, si no son gestionados adecuadamente, pueden socavar los beneficios esperados.

La implementación de infraestructuras de Big Data exige inversiones sostenidas en hardware, software, conectividad y ciberseguridad, así como la disponibilidad de personal especializado en ciencia de datos, estadística y tecnologías de la información (Camargo Vega et al., 2014).

En organizaciones militares con restricciones presupuestarias o con marcos normativos y administrativos rígidos, estos requerimientos pueden generar una brecha de capacidades entre quienes logran adoptar plenamente estas tecnologías y quienes solo alcanzan a incorporarlas de manera parcial.

Con respecto a la calidad y gestión de los datos, se pueden destacar aspectos no tan oportunos o favorables. Conjuntos de datos incompletos, desactualizados, sesgados o deliberadamente manipulados pueden conducir a conclusiones erróneas, incluso cuando se emplean algoritmos sofisticados.

Gandomi y Haider (2015) advierten que trabajar con grandes volúmenes de datos incrementa la probabilidad de correlaciones espurias y de interpretaciones equivocadas si no se aplican criterios de validación y métodos analíticos rigurosos. A su vez, la integración de fuentes heterogéneas (sensores militares, bases administrativas, redes sociales, imágenes satelitales comerciales) plantea desafíos de trazabilidad: no siempre es evidente el origen, el nivel de confiabilidad o las condiciones bajo las cuales fueron producidos esos datos.

La ausencia de políticas claras de calidad de datos y de mecanismos institucionalizados de revisión puede introducir sesgos sistemáticos en los productos de inteligencia, afectando la apreciación de la situación y el diseño de cursos de acción (Boyd & Crawford, 2012).

Aunque Big Data se presenta como una herramienta para aliviar la carga del analista, existe el riesgo de crear un entorno de sobrecarga informacional, caracterizado por una proliferación de productos, paneles, indicadores y alertas que el Estado Mayor no puede procesar de manera oportuna.

González Villegas (2024) y Haridas (2015) subrayan que, en estas condiciones, la saturación de información puede terminar por dificultar, en lugar de facilitar, la toma de decisiones, generando priorizaciones erráticas y dependencia creciente de atajos cognitivos.

En el nivel operacional, esto puede traducirse en dificultades para distinguir señales relevantes en medio del ruido y para alinear los productos de inteligencia con las necesidades efectivas del comandante.

Otro aspecto importante de destacar es que, las infraestructuras de Big Data, por su propia naturaleza conectada y distribuida, amplían la superficie de exposición a ciberataques, intrusiones y operaciones de manipulación de datos. Esto obliga a integrar la seguridad de la información, la ciberdefensa y la contrainteligencia como componentes inseparables del diseño e implementación de arquitecturas de Big Data en el ámbito militar.

Los desafíos y riesgos asociados a la integración de Big Data en la inteligencia militar muestran que su valor no reside únicamente en la disponibilidad de tecnologías avanzadas, sino en la capacidad institucional de regular, gobernar y emplear estas herramientas de manera responsable (Blanchard, Thomas & Taddeo, 2024).

La construcción de marcos doctrinarios, normativos y organizacionales sólidos resulta, por tanto, tan importante como la inversión en infraestructura y capacidades técnicas, si se busca que Big Data contribuya efectivamente a mejorar la calidad de la inteligencia y la toma de decisiones en los niveles táctico, operacional y estratégico.

Conclusiones parciales

Dado lo analizado en el presente capítulo, se puede inferir que;

La integración de Big Data en el proceso de inteligencia militar constituye una capacidad que transforma cualitativamente la producción de conocimiento en el nivel operacional.

El modelo de las “V” (volumen, velocidad, variedad, veracidad y valor) permite ampliar el horizonte de observación y sostener decisiones en contextos crecientemente complejos y acelerados.

La articulación de datos estructurados, semiestructurados y no estructurados muestra que el aporte de Big Data no reside solo en la acumulación de información, sino en su integración en un entorno analítico común, la cual fortalece todas las fases del ciclo de inteligencia.

La posibilidad de correlacionar datos procedentes de dominios físicos y no físicos permite comprender mejor las interdependencias del campo de batalla contemporáneo y apoyar procesos críticos como el targeting.

Desde la perspectiva de la toma de decisiones, las capacidades analíticas descriptivas, predictivas y prescriptivas asociadas a Big Data ofrecen un soporte robusto al comandante operacional.

Las herramientas de analítica de Big Data, tales como tableros (dashboards) integrados, modelos de tendencia y herramientas de optimización contribuyen a reducir la incertidumbre, anticipar riesgos y comparar cursos de acción sin reemplazar el juicio profesional, sino reforzándolo con evidencia más amplia y oportuna.

Las brechas de capacidades, los problemas de calidad y trazabilidad de los datos, la posibilidad de correlaciones espurias, la sobrecarga informacional y la mayor exposición a ciberataques pueden degradar la calidad de la inteligencia si no se cuenta con políticas claras en el tratamiento de datos, ciberseguridad y contrainteligencia.

Solo una integración acompañada de reformas organizacionales, desarrollo de competencias especializadas y adecuación doctrinaria permitirá que Big Data contribuya efectivamente a mejorar el análisis de inteligencia, por medio de su ciclo, y la toma de decisiones en los niveles táctico, operacional y estratégico.

Conclusiones

Del análisis realizado a lo largo del trabajo de investigación, puede inferirse que:

La articulación entre inteligencia de fuentes abiertas (OSINT) y Big Data mejora de manera tangible la gestión de la información y el análisis de inteligencia en apoyo a la toma de decisiones en el nivel operacional. Ambas herramientas contribuyen a reducir la brecha entre la abundancia de datos disponibles y la necesidad de producir inteligencia oportuna, pertinente y comprensible para el comandante.

La respuesta no reside en una única tecnología, sino en la convergencia de enfoques. La OSINT aporta método, criterios de validación y una mirada crítica sobre las fuentes abiertas, mientras que Big Data proporciona la capacidad técnica para procesar, integrar y explotar grandes volúmenes de datos heterogéneos.

La OSINT, tratada como disciplina y no como simple búsqueda en internet, refuerza cada fase del ciclo de inteligencia. Al ordenar, seleccionar y evaluar la información abierta, la OSINT permite que la dirección, obtención, procesamiento, análisis y difusión se orienten a las verdaderas necesidades del nivel operacional. De este modo, contribuye a la superioridad informacional y se proyecta sobre el dominio cognitivo y las operaciones multidominio.

Big Data amplía el horizonte analítico más allá del aumento de capacidad de almacenamiento. La posibilidad de integrar datos estructurados, semiestructurados y no estructurados en plataformas comunes habilita análisis descriptivos, predictivos y prescriptivos, que enriquecen la apreciación del ambiente operacional y la comparación de cursos de acción. Esto aporta profundidad y velocidad a los productos de inteligencia que recibe el Estado Mayor.

OSINT y Big Data sólo generan valor cuando se diseñan como un sistema integrado, centrado en datos y orientado a la misión. Las fuentes abiertas deben alimentar de forma continua las arquitecturas de Big Data, y estas, a su vez, devolver productos claros, priorizados y alineados con las necesidades esenciales de información del comandante.

Sin este enlace doctrinario, organizacional y tecnológico, el riesgo es pasar de la escasez de información a una nueva forma de saturación.

La integración de OSINT y Big Data en el proceso de inteligencia exige perfiles híbridos de analistas, que combinen el conocimiento doctrinario y operativo propio de la inteligencia militar con competencias en análisis de datos, estadística, manejo de herramientas digitales y comprensión de arquitecturas de información.

La inteligencia de fuentes abiertas (OSINT) y las capacidades de Big Data se integran de manera transversal al ciclo de inteligencia.

OSINT amplía la cobertura informativa, aporta contexto cualitativo y permite obtener información rápida y de bajo costo en todas las fases del proceso.

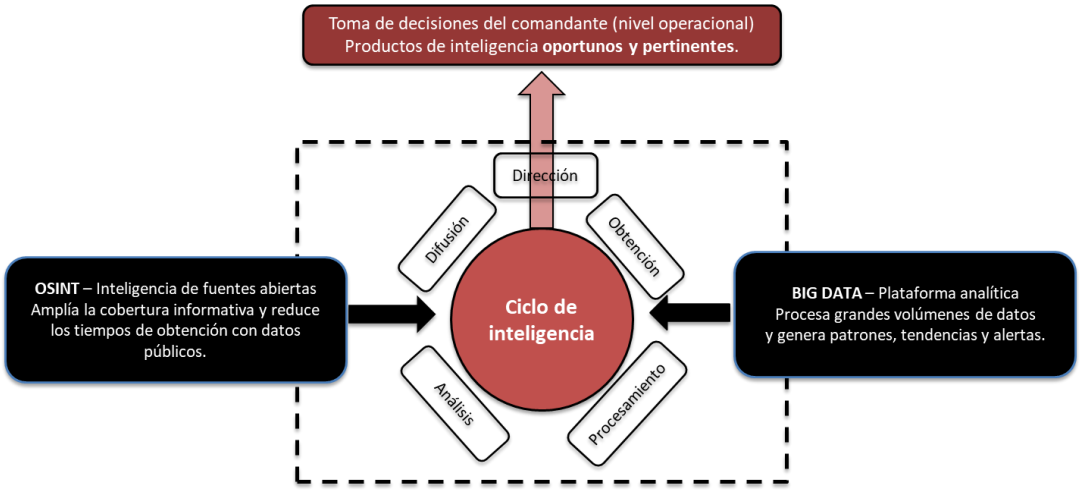
Big Data, por su parte, proporciona la infraestructura tecnológica y los métodos analíticos necesarios para gestionar grandes volúmenes de datos heterogéneos, mejorar su calidad, identificar patrones y generar visualizaciones útiles para la toma de decisiones.

La convergencia de ambas capacidades no sustituye el juicio del analista ni la conducción del comandante, pero sí aumenta la velocidad, la profundidad y la trazabilidad del ciclo de inteligencia, fortaleciendo el apoyo a la toma de decisiones en el nivel operacional.

A fin de reflejar gráficamente las utilidades de OSINT y Big Data, en el proceso de inteligencia en apoyo a la toma de decisiones, conforme las conclusiones extraídas, se expresa el siguiente gráfico.

Figura 4

Contribución de la OSINT y de Big Data a cada fase del ciclo de inteligencia en el nivel operacional.



Fase del ciclo	Aporte de OSINT	Aporte de Big Data
Dirección / Planeamiento	Proporciona un panorama inicial a partir de fuentes abiertas (medios, RRSS, documentos oficiales, think tanks, informes académicos), ayudando a delimitar las NEI y focalizar los requerimientos.	Explota grandes volúmenes de datos históricos (registros operacionales, logs, bases de eventos) para identificar patrones, tendencias y áreas críticas, aportando indicadores cuantitativos.
Obtención	Amplía el espectro de fuentes (medios, portales digitales, RRSS, sitios oficiales, bases públicas, repositorios académicos, imágenes comerciales), ofreciendo información rápida, de bajo costo y contextual.	Permite la ingesta masiva y automatizada de datos estructurados, semiestructurados y no estructurados (sensores, sistemas C2, registros logísticos, datos abiertos), integrándolos en una misma infraestructura.
Procesamiento	Depura, clasifica y verifica la información de fuentes abiertas, filtrando ruido, comprobando autenticidad y consolidando datos en bases o matrices analíticas.	Aplica procesos ETL (Extraer, Transformar y Cargar datos) a gran escala (limpieza, normalización, des duplicación e integración de fuentes), mejorando la calidad de los datos para el análisis.
Análisis	Aporta contexto cualitativo (narrativas, percepciones, discursos y comportamientos), contribuyendo a formular hipótesis, identificar tendencias y posibles cursos de acción.	Incorpora herramientas analíticas avanzadas (minería de datos, análisis de redes, detección de anomalías, modelos predictivos) que identifican patrones complejos, correlaciones y escenarios.
Difusión	Genera productos de inteligencia con ejemplos trazables desde fuentes abiertas y, mediante la retroalimentación, ajusta prioridades de temas y fuentes.	Proporciona visualizaciones dinámicas (dashboards, mapas, series temporales) y, mediante la retroalimentación, ajusta modelos, umbrales de alerta e indicadores.

Fuente: elaboración propia

Referencias bibliográficas

Arenas, J. (2021). *La organización de la jefatura de inteligencia del comando operacional de las Fuerzas Armadas en las operaciones multidominio*. Escuela Superior de Guerra Conjunta, Universidad de la Defensa Nacional.

Blanchard, A., Thomas, C., & Taddeo, M. (2024). *Ethical governance of artificial intelligence for defence: Normative tradeoffs for principle to practice guidance. AI & Society,* 185–198.

Bognár, E. K. (2020). *Novel IT Technologies on the Digital Battlefield: The Application of Big Data and Data Mining Technologies*. Hadmérnök

Boyd, d., & Crawford, K. (2012). *Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon*. Information, Communication & Society, 662–679.

Calvo Albero, G. J., & García Servert, F. (2021). *El dominio cognitivo en las operaciones multidominio: concepto y problemática* (Documento de Opinión 48/2021). Instituto Español de Estudios Estratégicos.

Camargo-Vega, J. J., Camargo-Ortega, J. F., & Joyanes-Aguilar, L. (2014). *Conociendo Big Data*. Sistemas & Telemática, 11–31.

Desclaux, G. (2018). *Big Data e Inteligencia Artificial para la toma de decisiones militares*. Documento de trabajo.

Ejército Argentino. (2015). *ROB 00-01 Conducción para las Fuerzas Terrestres.* Ciudad Autónoma de Buenos Aires: Departamento Doctrina.

Estado Mayor Conjunto de las Fuerzas Armadas. (2018). *PC 00-01 Doctrina básica para la acción militar conjunta*. Ministerio de Defensa.

Estado Mayor Conjunto de las Fuerzas Armadas. (2019). *PC 00-02 Glosario de términos de empleo militar para la acción militar conjunta*. Ministerio de Defensa.

Estado Mayor Conjunto de las Fuerzas Armadas. (2023). *IC-03-01 Concepción estratégica de "capas", restricción de áreas y de operaciones multidominio* (Boletín Informativo Conjunto, Año 2023). Estado Mayor Conjunto de las Fuerzas Armadas.

Felip i Sardà, J. (2004). *La gestión de fuentes abiertas*. En V. Iranzo Dosdad (Ed.), Manual de inteligencia (pp. 283–307). Plaza y Valdés.

Gandomi, A., & Haider, M. (2015). *Beyond the hype: Big data concepts, methods, and analytics*. International Journal of Information Management.

González Villegas, M. (2023). *Propuesta de un modelo conceptual de Big Data para la inteligencia militar*. Revista de Ensayos Militares. (72-86). Editorial:Tranviares

Haji Molla Mirzaie, H., Mohammadi, H., & Saadatmand, A. M. (2021). *Explain the role of "big data" technology in the intelligence of "cyber command and control" systems and providing its practical model*. Quarterly Journal of Interdisciplinary Studies on Strategic Knowledge.

Haridas, M. (2015). *Redefining military intelligence using Big Data analytics*. CLAWS Journal (Winter).

Hulnick, A. S. (2010). *The dilemma of open source intelligence: Is OSINT really intelligence?* En L. K. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 229–252). Oxford University Press.

King, A. (2024*). Digital targeting: Artificial intelligence, data, and military intelligence*. Journal of Global Security Studies,

Kulshrestha, S. (2016). *Big data in military information & intelligence*. SSRN Electronic Journal.

Las Heras, A., Díaz Monzón, L., & Blanco Torres, F. (2017). *El sesgo tecnológico en el análisis de inteligencia de fuentes abiertas*. Comunicación presentada en el XII Congreso Español de Ciencia Política y de la Administración, Asociación Española de Ciencia Política y de la Administración.

Lim, N., et al. (2019). *Leveraging big data analytics to improve military recruiting* (Research Report RR-2621). RAND Corporation.

Lowenthal, M. M. (2012). *Intelligence: From secrets to policy* (5.ª ed.). CQ Press.

Mana, D. (2018). *Capacidades, organización e interoperabilidad del Centro Integrador de Inteligencia, en apoyo a una Gran Unidad de Batalla para la toma de decisiones. Una propuesta*. Escuela Superior de Guerra del Ejército.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Eamon Dolan / Houghton Mifflin Harcourt.

Moore, D. T. (2007). *Critical thinking and intelligence analysis* (2.ª ed.). National Defense Intelligence College.

North Atlantic Treaty Organization. (2001). *NATO open source intelligence handbook*. NATO.

Pherson, R. H., & Pherson, K. H. (2016). *Critical thinking for strategic intelligence* (2.ª ed.). CQ Press.

Smallegange, J. A. P., Bastiaansen, H. J. M., Venema, A. P., & Bronkhorst, A. W. (2018). *Big data & artificial intelligence for military decision making: A Dutch perspective*. (pp. 43–56). Netherlands Defence Academy / TNO.

Treverton, G. F. (2001). *Reshaping national intelligence for an age of information*. Cambridge University Press.

Van Puyvelde, D., Coulthart, S., & Lennox, P. (2017). *Big data and national security decision-making: The role of intelligence*. International Affairs,

Williams, H., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise* (Research Report RR-1964-OSD). RAND Corporation.

Ziółkowska, M. (2018). *OSINT as a tool of military reconnaissance*. Security and Defence Quarterly.