# ¿Qué significa el crecimiento de la OSINT para los analistas de inteligencia militar?

*Marcel Plichta*
*Edwin Dudley-Taylor*
*Traducido al castellano por Daniel Blanco*

**Resumen**

La Inteligencia de Fuente Abierta (OSINT) está siendo adoptada por los profesionales de la inteligencia de todo el mundo y los analistas militares no son una excepción. Sin embargo, los analistas militares suelen responder a un conjunto distinto de requerimientos de información que sus homólogos en los servicios civiles y el sector privado. En consecuencia, las definiciones existentes de OSINT, así como sus ventajas y desventajas, pueden ser confusas y malinterpretadas en un contexto militar.

Este artículo definirá la OSINT en términos útiles para la inteligencia militar y analizará cómo las necesidades de los analistas y consumidores en contextos militares requieren conjuntos distintos de información. A continuación, se expondrán las ventajas y los desafíos de integrar significativamente la obtención de fuentes abiertas al proceso de inteligencia militar.

Además, se explorará como la OSINT ofrece a los analistas una forma adicional y, a menudo, más barata de responder a los requerimientos de los mandos, así como también facilita el intercambio de inteligencia con otros servicios de inteligencia y con el público en general. Pese a los beneficios, los analistas deberán evitar la dependencia excesiva de las fuentes abiertas en detrimento de los demás métodos de obtención y vigilar las posibles limitaciones legales y éticas en torno a la protección de datos.

**Palabras clave**

OSINT, Inteligencia militar, Analistas militares, Analistas de inteligencia, Fuentes abiertas.

## *What does OSINT growth mean for military intelligence analysts?*

**Abstract**

*Intelligence practitioners worldwide are embracing open-source intelligence (OSINT), and militaries are no exception. However, military analysts often answer a distinct set of questions compared to their counterparts in civilian intelligence and the private sector. Consequently, existing definitions of OSINT can be confusing, and the discipline's benefits and*

*tradeoffs are often misunderstood in a military context. In this article we will define OSINT in terms useful to military intelligence analysts and discuss how the needs of military analysts and consumers require a distinct set of information from OSINT. It will then draw out the benefits and challenges of adopting open-source collection more fully into the military intelligence process. Ultimately, OSINT collection offers an additional and frequently cheaper way for analysts to answer some kinds of intelligence questions and could make it easier to share intelligence with other services and the general public. At the same time, analysts should be wary of overreliance on OSINT to the exclusion of other collection disciplines, consumer bias towards or against information collected from OSINT, and the potential legal and ethical constraints for collecting personal information.*

**Keywords**

*OSINT, Intelligence analysis, Military intelligence, Intelligence training, Tradecraft.*

## 1 Introducción

Durante los últimos años, las organizaciones de inteligencia han realizado un esfuerzo concertado para adoptar e integrar la inteligencia de fuentes abiertas (OSINT) a su trabajo. Diversos académicos comentan que los países del hemisferio occidental —en particular— podrían beneficiarse de ello. Harper y Cross, por ejemplo, afirmaron en 2024 que la OTAN puede «adelantarse, disuadir y derrotar los esfuerzos de sus adversarios mediante la explotación de la inteligencia de fuentes abiertas» (Harper y Cross, 2024). La Oficina del Director de Inteligencia Nacional de Estados Unidos (ODNI) fue un poco más lejos y calificó a la OSINT como «la inteligencia de primer recurso» en su Estrategia OSINT 2024-2026 (ODNI, 2024).

Pese a que la adopción de OSINT promete mejoras, que van desde una mejor obtención de inteligencia hasta una reducción de costes operacionales, sus beneficios generan preguntas entre los analistas militares y sus respectivas instituciones. Este artículo busca analizar las ventajas y los desafíos de dar prioridad al OSINT en la obtención de información dentro de contextos militares. «¿Qué implica el crecimiento de la OSINT para los analistas de inteligencia militar?», comenzará con una visión general de la inteligencia de fuentes abiertas y de los elementos únicos que caracterizan a la inteligencia militar. Seguidamente, el artículo analizará las ventajas de la OSINT para los analistas militares y los posibles obstáculos a los que se enfrentarán a la hora de incorporar los métodos de fuente abierta a su trabajo.

La OSINT ofrece a las organizaciones con competencias de inteligencia militar una nueva vía para responder a sus requerimientos de información y coordinarse con otras instituciones, pero también plantea retos que van desde garantizar que los consumidores de inteligencia y tomadores de decisiones comprendan los límites de la disciplina, hasta asegurar que los procesos de obtención sean realizados dentro de los límites legales. Cualquier grado de utilidad que los analistas militares puedan sacar de esta disciplina, será determinado por la forma en que las organizaciones afronten los desafíos planteados por las fuentes abiertas.

## 2 ¿Qué es OSINT?

Aunque el debate sobre OSINT está creciendo astronómicamente en los círculos de inteligencia, tanto las agencias gubernamentales como los expertos académicos utilizan el término para referirse a conceptos diferentes, a menudo con definiciones intercambiables. Por ejemplo, las empresas privadas y las organizaciones no gubernamentales pueden utilizar OSINT para referirse a cualquier trabajo del sector privado relacionado con la inteligencia, como las auditorías externas, las investigaciones privadas, la seguridad personal, los asuntos públicos o el periodismo de

investigación. Otros conceptos más estrictos la emplean como una abreviatura de la inteligencia derivada, en concreto, de las plataformas de medios sociales, mientras que la definición más laxa recae en los agregadores de contenido en redes sociales, que califican tareas sencillas de cotejo de información como «OSINT».

Para complicar las cosas, la OSINT también es un término que engloba diferentes actividades de obtención de información, algunas de las cuales se solapan con disciplinas ya establecidas. Por ejemplo, el uso de imágenes de satélites comerciales para observar la actividad en una base militar es GEOINT por definición, pero también es considerado OSINT si las imágenes recaen en el ámbito de la información disponible públicamente. Desde el punto de vista organizativo, esto significa que un analista de GEOINT podría ser también un analista de OSINT aunque esté aplicando el mismo conjunto de conocimientos en disciplinas diferentes.

Asimismo, los funcionarios gubernamentales también utilizan definiciones diferentes, refiriéndose en ocasiones a la OSINT como productos de inteligencia elaborados con información disponible públicamente. La OSINT suele ser definida a nivel de Gobierno como una disciplina de obtención, como la HUMINT y la SIGINT. El Centro Nacional de Inteligencia de España describe OSINT como «información procedente de fuentes abiertas». La Oficina del Director de Inteligencia Nacional de Estados Unidos, por su parte, publicó una definición actualizada de OSINT en diciembre de 2024 que la definía como una disciplina «derivada exclusivamente de información pública o comercialmente disponible» (ODNI, 2024: 6). Esto contrasta con su descripción de los productos de inteligencia OSINT, que son «derivados exclusivamente de PAI, CAI o OSINT» (ODNI, 2024: 7).

Durante el resto de este artículo se entenderá la OSINT como una *actividad de obtención*. Esto no significa que la OSINT carezca de relevancia para los analistas, sino todo lo contrario. Como se verá más adelante, la recopilación de información de fuentes abiertas alimenta de forma natural el procesamiento y el análisis de los productos de inteligencia.

## 3 Prioridades de la inteligencia militar y civil

Buena parte de los debates académicos sobre OSINT se centran en su utilidad en contextos civiles, ya sea en el sector privado o en una agencia de inteligencia de carácter civil. No obstante, los consumidores de inteligencia militar y los consumidores de inteligencia civil tienen diferencias importantes. Ambos tienen requerimientos de información y preferencias analíticas distintas, así como funciones que apoyan actividades conjuntas con propósitos diferentes, incluso si ambos consumidores forman parte del mismo Gobierno.

La inteligencia militar incluye entre sus consumidores a los responsables de tomar decisiones en las fuerzas armadas, como los comandantes de los ejércitos, los responsables políticos civiles que dirigen o asesoran sobre la política de defensa o los líderes nacionales que dirigen a las instituciones militares, mientras que los servicios de información civiles suelen abarcar una amplia gama de cuestiones de inteligencia, que van desde la estabilidad económica hasta la seguridad cibernética, la inteligencia militar suele ser más restrictiva. Dado que el comercio, la diplomacia o la delincuencia no forman parte del núcleo fundamental de la inteligencia militar —a menos que representen una amenaza para la defensa nacional— los analistas de inteligencia en instituciones armadas suelen centrar sus esfuerzos en las intenciones de adversarios, la lucha antiterrorista y las operaciones militares.

El uso principal de la inteligencia militar en un contexto estratégico es la planificación operacional o la prospectiva de defensa. Aunque en algunas ocasiones —como en la seguridad nacional— se produce un solapamiento entre la inteligencia militar y los servicios civiles, los analistas, normalmente, suelen adoptar enfoques adaptados a las diferentes necesidades de sus consumidores. Al igual que los servicios de información civiles, las organizaciones de inteligencia militar realizan diversas actividades de obtención. Además de la Inteligencia de Fuentes Abiertas, suelen incluir disciplinas de recopilación más antiguas, como la Inteligencia de Señales, la Inteligencia Humana y la Inteligencia Geoespacial. Dependiendo de cómo estén estructuradas las comunidades de inteligencia en los organigramas nacionales, las agencias civiles también pueden estar bajo el mismo paraguas general que las instituciones militares, como es el caso de la Agencia de Seguridad Nacional de Estados Unidos.

Pese a que los organismos militares y servicios civiles comparten el mismo acervo de información, los analistas de inteligencia de los ejércitos destinan el proceso de obtención a fines diferentes. Los productos de inteligencia militar se centran en «apoyar a los mandos en su toma de decisiones, ayudándoles a aumentar su comprensión», lo que puede abarcar desde las evaluaciones de amenazas a corto plazo hasta necesidades a más largo plazo como la previsión estratégica (*Ministry of Defence*, 2023: 8-9). La inteligencia militar suele evaluar temas como las capacidades de las fuerzas contrarias, la probabilidad de un conflicto y los retos para las operaciones planificadas o en curso.

La inteligencia militar a largo plazo también se utiliza en la política de defensa, el desarrollo de armamento y el análisis geopolítico para anticiparse a las amenazas emergentes y mantener o alcanzar la superioridad militar de una nación. Las necesidades de los consumidores de inteligencia militar requieren un conjunto único de productos de los analistas de inteligencia. Por ejemplo, los analistas militares suelen elaborar análisis del

orden de batalla, evaluaciones de daños en batalla y reportes de selección de objetivos que responden a las necesidades específicas de los comandantes del campo de batalla y los responsables de la toma de decisiones (USMC, 2016). Mientras que algunos beneficios del OSINT son intercambiables entre el ámbito civil y el entorno militar, los desafíos que se presenten en este último serán determinados por la medida en la cual la obtención de información de fuente abierta facilite o dificulte la elaboración de análisis para consumidores de defensa.

## 4 Ventajas de la OSINT para los analistas militares

Aunque los analistas militares se enfrentan a una serie de requisitos y expectativas diferentes a los de sus homólogos civiles, la OSINT ofrece formas de mejorar sus análisis y facilitar su difusión. Por ejemplo, los analistas podrían aprovechar la OSINT para subsanar vacíos de información y verificar fuentes de otras disciplinas, así como evaluar distintos medios de obtención y facilitar el intercambio de inteligencia con otras organizaciones.

Sobre el proceso de obtención, cabe destacar que su función principal es recolectar información destinada a producir inteligencia que pueda responder las preguntas de los consumidores finales. Durante la aplicación de este proceso pueden surgir lagunas o vacíos que dejen a los analistas militares y tomadores de decisiones con una imagen incompleta del asunto a evaluar. La OSINT podría llenar algunas de las brechas mencionadas con anterioridad.

Para ilustrar el argumento, se puede mencionar que la estrategia de propaganda y reclutamiento de un grupo extremista podría ser difícil de entender sin un esfuerzo coherente por recopilar sus declaraciones públicas y mensajes oficiales en las redes sociales. Adicionalmente, estudiar las métricas de interacción que obtienen estos mensajes podría ayudar a determinar su grado de eficacia.

Por otra parte, la recopilación de información en las redes sociales, como imágenes de combate, puede ayudar a los analistas a comprender dónde se están produciendo los combates con mayor precisión y rapidez que otros métodos de recopilación en las circunstancias adecuadas. Aunque la sobreabundancia informativa podría afectar de manera negativa a los analistas, un volumen mayor de fuentes abiertas puede ayudar a reforzar la evidencia en las cual basan sus conclusiones. Las Fuerzas Armadas de los Estados Unidos descubrieron a través de sus investigadores que la OSINT puede ayudar a los analistas a «identificar despliegues, movimientos, ejercicios, objetivos y disposiciones inusuales, seguimiento de objetivos de alto valor y patrones logísticos inusuales» (Sieting, 2024).

Como ejemplo reciente una base del Grupo Wagner fue geolocalizada y atacada por el Ejército de Ucrania después de que un periodista subiera una foto del sitio a sus redes sociales (Kirichenko, 2023). La OSINT también puede contribuir a la evaluación de daños y bajas (BDA) o al análisis del orden de batalla (ORBAT) en caso en que haya imágenes del combate o de sus consecuencias en las redes sociales; este tipo de análisis lo intentan a menudo las empresas de inteligencia que desarrollan sus actividades en el sector privado, lo que indica que los métodos de OSINT podrían aumentar la pluralidad de la información que el personal militar necesita para mantener y presentar el orden de batalla (ORBAT) actualizado que requieren sus consumidores (Jane, 2024). Aunque los analistas militares sigan dependiendo, en gran medida, de otras disciplinas de obtención para producir inteligencia, un flujo adicional de información procedente de los recopiladores OSINT mejorará la confianza de los analistas y añadirá redundancia si se pierde una fuente de información.

Centrarse más en la obtención de OSINT significa también que los analistas militares podrían operar mejor en entornos conflictivos o restrictivos donde otros métodos de obtención podrían no funcionar. La naturaleza descentralizada de la información de fuente abierta, que a menudo es compartida de forma voluntaria por muchas personas diferentes, la convierte en una fuente flexible en las circunstancias adecuadas. Ramsey (2024: 7) señala que, en lugares donde se dificulta a la obtención de información por parte de plataformas nacionales, «la OSINT probablemente estará disponible debido al gran número de sensores que proporcionan información y que probablemente también servirán como recurso principal para cubrir estas lagunas». Existen límites a la información que puede ser recopilada en un contexto de batalla, en especial, si un beligerante impone un apagón de comunicaciones u alguna otra medida para controlar la información en el área de operaciones. Aun así, el acceso a la OSINT podría ser un salvavidas para los analistas militares con fuentes limitadas de información.

Mediante la recopilación de publicaciones nacionales y prensa extranjera en redes sociales, la OSINT también puede ayudar a determinar las intenciones de los adversarios respecto a su percepción de la opinión pública. Por ejemplo, una nación adversaria podría amplificar la idea de que su tecnología de misiles puede vencer las defensas aéreas de un vecino. El Cuerpo de la Guardia Revolucionaria Iraní, de acuerdo con distintos reportes, invierte fuertemente en plataformas comunicacionales para «controlar parte del proceso de influencia en Irán, asegurando que su narrativa estratégica y su percepción de la realidad sigan siendo dominantes» (Gill, 2020: 113). Como segundo ejemplo, una organización extremista podría hacer públicas sus amenazas para causar pánico y ejercer presión a las autoridades locales. Los analistas pueden interpretar los mensajes estratégicos a través de

fuentes abiertas para conocer las intenciones o prioridades de un adversario, aunque, como se verá más adelante, deben ser de igual modo conscientes del engaño y la desinformación en las fuentes abiertas.

## 5 La utilización de la OSINT para mejorar y verificar la obtención

Se debe precisar que otros métodos de obtención suelen llenar las mismas lagunas de información que las fuentes abiertas. La HUMINT podría describir una estrategia de propaganda a través de una fuente clasificada y la GEOINT podría indicar con exactitud la región dónde se están produciendo los combates o ayudar con el análisis del orden de batalla. Ahora bien, los defensores de la OSINT sostienen que es una forma más rentable de responder a las mismas preguntas de los consumidores de inteligencia. Por ejemplo, los requerimientos de información de una agencia gubernamental pueden no necesitar una costosa plataforma satelital si existe un proveedor comercial con las mismas capacidades.

Conviene señalar, sin embargo, que el potencial ahorro de costes operativos no es percibido directamente por los analistas. Como mucho, podría significar que sus productos son diferentes, pero no necesariamente mejores si llegan a la misma conclusión analítica. Por supuesto, los responsables políticos o los directores de las instituciones pueden decidir que, de todos modos, merece la pena el esfuerzo de construir y mantener capacidades de obtención propias, sin importar su presupuesto. Incluso en esos casos, la OSINT podría ayudar a triangular y rellenar las lagunas dejadas por la información fragmentaria. Miguel Sánchez de Toca Alameda et al (2023: 21) señalan que la OSINT puede «apoyar a otras disciplinas de inteligencia para confirmar o desechar hipótesis» en un contexto militar.

Esto beneficia la confianza de los analistas en sus evaluaciones, así como su capacidad para ofrecer información a los operadores de las demás disciplinas. Gracias a la obtención de información de fuente abierta, los analistas pueden, por ejemplo, hacer un seguimiento de la información incompleta procedente de una fuente humana para confirmar la exactitud de la información. Esto, a su vez, mejora la capacidad de los analistas de HUMINT para evaluar la calidad o credibilidad de las fuentes empleadas en el proceso de obtención.

La OSINT también podría incrementar el alcance de las organizaciones con recursos limitados. En los últimos años, las herramientas de código abierto han permitido desde rastrear envíos internacionales hasta determinar interferencias en sistemas de posicionamiento satelital. Por ejemplo, Grey Dynamics ayudó al canal de televisión CBS News a rastrear las actividades ilícitas del Grupo Wagner en África Central mediante el empleo de métodos de fuentes abiertas. (Grey Dynamics, 2024)

Mientras que en la era pre-Internet resultaba difícil y costoso vigilar los acontecimientos mundiales, la información y las herramientas disponibles en la actualidad para los encargados de la obtención facilitan considerablemente el análisis a quienes carecen de herramientas de obtención más avanzadas, como aquellas disponibles en los servicios de información o agencias de inteligencia del sector público.

También se debe recordar que todas las organizaciones de inteligencia no siempre cuentan con los recursos y capacidades de agencias grandes como la CIA o la DGSE; las naciones más pequeñas pueden estar interesadas solo en obtener información sobre su región inmediata o pueden carecer del presupuesto para ejecutar operaciones clandestinas de obtención. Sin embargo, las amenazas para un país y sus ciudadanos no siempre son próximas. Como ejemplo, se presentan los buques comerciales de un actor estatal. Estos pueden atravesar o acercarse a una zona de conflicto situada a miles de kilómetros de sus fronteras. Incluso si el buque está fuera del alcance de los elementos operativos de los servicios de información, los responsables políticos pueden dar instrucciones a la inteligencia militar para que evalúe la seguridad de las embarcaciones. Para satisfacer rápidamente los requerimientos de información, los analistas militares podrían contratar los servicios de una empresa o la licencia de una herramienta que se especialice en la obtención de fuentes abiertas. Esto aumenta el rango de la información disponible para los analistas de inteligencia.

## 6 Uso de OSINT en transparencia e intercambio de inteligencia

La inteligencia militar también puede aprovechar la OSINT para mejorar la transparencia de sus procesos. Aunque el trabajo de los servicios de información suele ser clasificado y opaco por motivos de seguridad nacional, las instituciones gubernamentales pueden aumentar la confianza de la ciudadanía en su trabajo mediante la publicación de sus productos de inteligencia y conclusiones analíticas, siempre que sea posible. La OSINT juega un papel fundamental en dicha estrategia, ya que la información abierta puede desclasificarse con un riesgo menor en cuanto a la revelación de material sensible o métodos clasificados. La Agencia de Inteligencia de Defensa de Estados Unidos publicó en 2023 un informe con información de fuentes abiertas para demostrar que Rusia estaba utilizando drones diseñados por Irán en Ucrania (DIA, 2023).

Asimismo, los productos provenientes de OSINT también pueden facilitar el intercambio de inteligencia con aliados y socios debido a su naturaleza de fuente abierta. El proceso de desclasificar información o hacerla accesible a un Gobierno aliado suele ser laborioso, sobre todo, si el producto de inteligencia utiliza diversas fuentes para sustentar análisis. Mientras que un servicio o departamento de inteligencia militar puede guardar celosamente

sus métodos de obtención más sensibles, un producto que se base en su mayor parte o en su totalidad en OSINT sería más fácil de compartir con un socio en el que la agencia no confíe plenamente con la seguridad operacional de sus fuentes. Una filtración o filtración de productos de inteligencia basados en información abierta, sin dejar de ser una amenaza para la seguridad nacional, es más segura y menos comprometedora que la filtración de la identidad de una fuente humana o los detalles técnicos de una plataforma de señales.

## 7 Retos para los analistas militares

La OSINT puede ofrecer oportunidades para rellenar vacíos en los requerimientos de información o triangular información de fuentes provenientes de métodos de obtención distintos, pero también presenta límites y desafíos. Entre los retos a los cuales podrían enfrentarse los analistas militares se encuentran cantidades abrumadoras de información y operaciones de engaño por parte de los adversarios, así como los prejuicios del consumidor, el aumento de la privatización y las restricciones legales en las plataformas abiertas.

Romanow señala que «los mismos sesgos analíticos que han alimentado los fallos de inteligencia en el pasado seguirán estando presentes e incluso podrían acentuarse por las muchas nuevas fuentes y los nuevos actores en el campo de la inteligencia militar» (2025). Asegurarse de que se abordan estos inconvenientes es primordial para garantizar que los analistas militares puedan sacar el máximo provecho de las fuentes abiertas.

Quienes desempeñen labores analíticas, no deben asumir que la inteligencia de fuentes abiertas rellenará por sí misma los vacíos de *data*. Tampoco deben de sentirse presionados para recurrir a las fuentes abiertas a expensas de los demás métodos de obtención. La OSINT, como todas las disciplinas de inteligencia, puede no responder a los requerimientos de información más específicos de las instituciones militares Esto ocurre debido a que la inteligencia militar busca reunir información sobre las capacidades e intenciones de los ejércitos adversarios, información que no siempre está disponible en fuentes abiertas.

Por ejemplo, la localización de las bases aéreas de un país adversario puede ser información de dominio público, pero una lista de los recursos o activos militares presentes en esas localizaciones seguramente será clasificada. Del mismo modo, las fuentes abiertas no pueden reemplazar actividades de obtención en elementos restrictivos, como la intervención de las señales de una organización extremista para monitorear sus comunicaciones.

Otro de los mayores desafíos en la obtención de información de fuentes abiertas, es la incoherencia de los «sensores». Quienes agregan contenido

en redes sociales podrían indicar dónde se encuentra una unidad adversaria hoy, pero no mañana. Otras cuentas podrían, por confusión o impericia, etiquetar de forma errónea ubicaciones y acontecimientos o incluso afirmar que vídeos antiguos corresponden a acontecimientos recientes. Esto se agrava en un contexto militar, donde el público civil suele identificar incorrectamente el material militar, como ilustró el vídeo viral difundido por los rebeldes sudaneses el 21 de noviembre 2023, que mostraba una plataforma de defensa antiaérea Pantsir-S1 rusa y resultó ser falso (*Army Recognition*, 2023). La cuestión de la fiabilidad no es exclusiva de la OSINT, pero añade otro nivel de complicaciones para los analistas militares que deben asegurarse sin cesar de que utilizan información de calidad en sus productos.

Todos los métodos de obtención son susceptibles al engaño. La OSINT, sin embargo, presenta un problema considerable —en particular, con la información en redes sociales— para los servicios de inteligencia. Existen algunos factores que complican la situación ya descrita, en primer lugar, los usuarios de las redes sociales no suelen sentir la necesidad de comprobar o verificar el contenido o las afirmaciones que comparten. Esto significa que, aunque los usuarios no tengan intención de engañar, pueden hacerlo por falta de rigurosidad.

Todavía más complicado es el creciente problema de la desinformación difundida a propósito por agentes malignos o programas automatizados. Confiar en la recolección de datos de las redes sociales es, por tanto, complicado para los analistas, ya que los usuarios y las publicaciones pueden tener una relación endeble con la realidad objetiva. Para los analistas militares, el volumen de información y el alcance de los engaños pueden reducir la utilidad de las fuentes abiertas en el contexto de un campo de batalla.

Rasak (2021: 52) señala que «las consecuencias del bombardeo de eventos, las campañas de desinformación, el secuestro de tendencias y el engaño militar restarán fundamentalmente utilidad a la OSINT a nivel táctico». Puede que los mandos no deseen tomar una decisión importante en el campo de batalla basándose en un flujo de información comprometido, y que los analistas no difundan sus conclusiones hasta que haya una confirmación independiente de los datos obtenidos. Estos problemas pueden hacer que los productos de inteligencia basados en OSINT sean menos accionables y también socavan una de las ventajas pregonadas de la OSINT, que a menudo suele ser la velocidad en sus flujos de información.

Pese a los desafíos ya mencionados, la recopilación de información en las redes sociales es beneficiosa para las organizaciones militares que necesitan comprender y contrarrestar los efectos de la desinformación o la información errónea. Anticipar el impacto de la desinformación es vital porque, aunque algo no sea cierto, las personas pueden ajustar su comportamiento si catalogan la información falsa como un evento cierto.

Por ejemplo, las imágenes manipuladas de unas maniobras militares al otro lado de la frontera podrían incitar a un comandante a poner a sus fuerzas en alerta. Comprender los orígenes y las intenciones (si las hay) del engaño a través de las redes sociales es, por tanto, una poderosa forma de que los analistas informen a los responsables de la toma de decisiones. Comprender los orígenes y las intenciones (en caso de que las haya) de las operaciones de engaño a través de las redes sociales es, por tanto, una herramienta poderosa para que analistas informen a los responsables de la toma de decisiones.

Otro problema relacionado a la OSINT es que los consumidores de inteligencia pueden tener prejuicios en contra o a favor de las fuentes abiertas, debido a que suelen tener opiniones personales sobre qué métodos de obtención son más fiables. Como ejemplo, un general podría considerar que la información recopilada en redes sociales no es lo suficiente fiable como para llevar a autorizar una operación. Por otro lado, un consumidor de inteligencia podría dar prioridad a la OSINT sobre un asunto no necesariamente adecuado, solo porque cree que la obtención de fuentes abiertas es menos costosa en términos operativos.

Estos sesgos personales se agravan en los servicios de inteligencia si se agrega inteligencia artificial (IA) al procesamiento de datos. Juan Luis Sánchez Sánchez (2025: 19) sostiene que «el empleo creciente de la IA para analizar el entorno de la información mediante OSINT será fundamental para prevalecer y adelantar escenarios de inteligencia para el posterior empleo defensivo/ofensivo». Para los analistas militares, esto significa desarrollar nuevas habilidades para sacar el máximo partido de la inteligencia artificial y desarrollar una comprensión rudimentaria de cómo funcionan las IA y, en particular, los LLM (modelos de lenguaje de gran tamaño) para protegerse de problemas como las alucinaciones.

Sin embargo, no hay mucho que los analistas puedan hacer, ya que en gran medida estarán a merced de la organización de inteligencia más amplia que dicta dónde y cómo se utiliza la IA en el ciclo de inteligencia. Cualquiera de estas situaciones puede convertirse en un reto para los analistas militares, que tienen que asegurarse de que están caracterizando adecuadamente sus fuentes en los productos de inteligencia y en las sesiones informativas.

## 8 Restricciones legales y privatización de la obtención

Incluso en un contexto gubernamental, el debate sobre OSINT a menudo se solapa con la aparición de contratistas privados y empresas tecnológicas. La incorporación de contratistas de inteligencia podría representar una manera inicial de integrar a las entidades privadas a las instituciones

gubernamentales, debido a que los métodos de obtención de fuente abierta no suelen ser clasificados y los especialistas de la disciplina no necesitan necesariamente habilitaciones de seguridad tan elevadas como si trabajaran con otros métodos de obtención.

Si la empresa contratista ya cuenta con la capacidad y el personal necesarios, su incorporación a un servicio de inteligencia gubernamental podría resultar más rápido y asequible para los responsables políticos que crear una capacidad interna de características similares desde cero. Sin embargo, la privatización de la obtención plantea sus propios retos a los analistas. Williams y Blum (2018: 22-23) señalan que los productos comerciales tienen costes ocultos para los gobiernos, ya que deben adaptarse a sistemas clasificados.

Desde un punto de vista de seguridad, las naciones más pequeñas podrían tener que arriesgarse a contratar a una empresa extranjera o contratista multinacional para que les proporcione los servicios OSINT que desean en sus servicios de información. Ambas cuestiones pueden complicar el trabajo de los analistas militares y los funcionarios públicos, que podrían acabar lidiando con un proceso complicado de acceso a la información recopilada o perdiendo el acceso a las herramientas de obtención si la empresa pierde o no renueva su contrato con el Gobierno.

Por otro lado, el debate sobre la privatización de la OSINT también se solapa con otra consideración clave: las restricciones éticas o legales a la recopilación de información en el dominio público (Smith y Cook, 2023). Aunque un miembro del público ponga su información en Internet, las agencias de inteligencia pueden, sin que sea necesario, tener acceso a su obtención, debido a las leyes que regulan la recopilación y el almacenamiento de datos personales, sobre todo, en las naciones democráticas del hemisferio occidental.

Los analistas militares suelen centrarse en las amenazas externas más que en los asuntos internos, pero aun así tienen que asegurarse de que trabajan dentro de la legalidad en casos como el de un ciudadano que actúa en el extranjero o cuestiones como la contrainteligencia doméstica. Al igual que en el caso de la inteligencia artificial, los límites legales y las decisiones contractuales de la OSINT están en gran medida fuera del alcance de los propios analistas, pero siguen siendo un impedimento potencial para su trabajo si se aplican de forma ineficaz.

La privatización añade una capa más a los desafíos legales y éticos mencionados, ya que las empresas pueden enfrentarse a un complicado conjunto de normativas locales para ejecutar la obtención, especialmente si no tienen su sede en el mismo país que el servicio de inteligencia que los contrata. Proelium (2024), un bufete de abogados británico, señala que «la

posición jurídica general es que la [Ley de Inteligencia del Reino Unido] no se aplica a las actividades de una empresa privada, sin embargo, esa posición es diferente cuando una empresa privada es contratada por una entidad gubernamental para llevar a cabo una actividad equivalente a actividades de vigilancia». Debido a ello, los analistas que trabajan con empresas privadas para recopilar OSINT podrían acabar obteniendo menos información de la prevista para cumplir las leyes y acuerdos locales.

## 9 Conclusiones

Nuestro estudio analizó las ventajas y desafíos relacionados al empleo del OSINT en la inteligencia militar. La implicación principal es la necesidad de que los responsables políticos y tomadores de decisiones de las instituciones correspondientes comprendan las implicaciones de integrar fuentes abiertas a la inteligencia militar. Aunque, por lo general, se considera que la OSINT es una de las disciplinas de obtención con menor coste, desarrollar herramientas y capacidades supone una inversión significativa de recursos que luego podrían acabar infrautilizados y malgastados.

Para los propios analistas, es imperativo entender cómo integrar la OSINT a sus flujos de trabajo de manera efectiva. Dado que las herramientas y metodologías de OSINT pueden afectar a una amplia gama de actividades analíticas, los analistas deben asegurarse de que han recibido la formación adecuada para aprovechar las ventajas de las fuentes abiertas sin sucumbir a los inconvenientes ya conocidos de las fuentes abiertas, como la saturación de información.

También existen oportunidades para que los académicos y profesionales del sector de la inteligencia amplíen el debate sobre dónde puede la OSINT mejorar el análisis de inteligencia para las instituciones militares. Pese a que las fuentes abiertas suelen estudiarse de manera aislada, en los círculos de inteligencia y en los sectores de seguridad es necesario explorar más a fondo las formas en que las fuentes abiertas podrían mejorar la inteligencia militar y cubrir vacíos de información. Además, se podría ampliar el debate entre las fuentes abiertas y la inteligencia artificial.

Por último, la OSINT cambiará la forma de trabajar de los analistas militares a medida que se incrementa su empleo y dependencia, con contextualización adecuada y el apoyo institucional, por lo que puede convertirse en una herramienta poderosa para las fuerzas gubernamentales. Queda por ver hasta qué punto muchos de los conocimientos básicos que utilizan los analistas de inteligencia tienen menos relación con los métodos de obtención y más con el pensamiento crítico, la anticipación a las necesidades de los consumidores de inteligencia y la entrega rápida de sus conclusiones analíticas.

Pese a que no hay duda de que la OSINT podría ayudar a llenar vacíos de información y acelerar la llegada de inteligencia crítica, los analistas militares deben asegurarse de que la OSINT se trata con el mismo nivel de seriedad y escrutinio que otras disciplinas de obtención, sobre todo, por la importancia que supone la inteligencia militar para asuntos críticos relacionados con la seguridad nacional.

## Bibliografía


Defense Intelligence Agency. (2023). *Iranian UAVs in Ukraine: A Visual Comparison*. Defense Intelligence Agency.

Gill, M. (2020). Capitalism, Communications, and the Corps: Iran's Revolutionary Guard and the Communications Economy. NATO Strategic Communications Centre of Excellence, p. 113.

Grey Dynamics. (2024). Case Studies [en línea]. Central Africa. [Consulta: 2025]. Disponible en: https://greydynamics.com/case-studies/

Harper, C. y Basset Cross, R. (2024). NATO Must Recognize the Potential of Open-Source Intelligence [en línea]. Atlantic Council. [Consulta: 2025]. Disponible en: https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-potential-of-open-source-intelligence/

Kirichenko, D. (2003). The Growing Use of Scamming Techniques and Social Media on the Battlefield [en línea]. Irregular Warfare Center. [Consulta: 2025]. Disponible en: https://irregularwarfarecenter.org/publications/perspectives/the-growing-use-of-scamming-techniques-and-social-media-on-the-battlefield/

Ministry of Defence (UK). (2023). Joint Doctrine Publication 2-00. Intelligence, Counter-Intelligence and Security Support to Joint Operations. Gov.uk, pp. 8-9. [Consulta: 2025]. Disponible en: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf

Office of the Director of National Intelligence. (2024). Citation and Reference for Publicly Available Information, Commercially Available Information and Open Source Intelligence. Office of the Director of National Intelligence.

Office of the Director of National Intelligence. (2024-2026). *The Intelligence Community OSINT Strategy*. United States Intelligence Community.

Proelium (2024). Compliance in OSINT: Legal Requirements for Data Protection and Privacy [en línea]. Proelium. [Consulta: 2025]. Disponible en: https://proeliumlaw.com/open-source-intelligence-and-privacy/

Ramsey, C. (2024). Ivy Intelligence (IVI) Large-Scale Combat Operations Targeting. *Military Review. The Professional Journal if the U.S. Army*, p. 7

Rasak, J. (2024). Event Barraging and the Death of Tactical Level Open-Source Intelligence [en línea]. Army University Press. [Consulta: 2025]. Disponible en: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Rasak-Open-Source-Intelligence-1.pdf?ver=OQwPyC0UYip2VkQsWIS7dQ%3D%3D

Romanow, N. (2025). The Transparency Trap: Risks of Deception in the Age of OSINT. *Proceedings*. U.S. Naval Institute. 151(1), p. 1463.

Sánchez Sánchez, J. L. (2025). Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias. *Documento Analísis 09/2025*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, p. 19.

Sieting, L. (2024). Intelligence Discovery Experiment Open-Source Intelligence Support to Targeting. Military Intelligence.

Smith, A y Cook, S. (2023). Guide to Open-Source Intelligence [en línea]. Grey Dynamics. [Consulta: 2025]. Disponible en: https://greydynamics.com/a-guide-to-open-source-intelligence-osint-2/

Sánchez de Toca Alameda, M., Díaz, J., Martín, R. y Muñoz, A. (2023). El Subsistema De Inteligencia Del Ejército De Tierra: Presente Y Retos De Futuro. *Cuaderno de Inteligencia*. Madrid, Ministerio de Defensa, p. 21.

United States Marine Corps (2016) Doctrinal Publication 2, Intelligence, and Marine Corps Warfighting: Intelligence Operations Intelligence Production and Analysis. *MAGTF Intelligence Production and Analysis*. U.S. Marine Corps.

Williams, H. y Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. *Rand*. Santa Mónica, Rand Corporation, pp. 22-23.