



TRABAJO FINAL DE CURSO (TFC)

ARTÍCULO DIVULGATIVO

**DEPARTAMENTO DE INTELIGENCIA
CTE. D. Pedro Ramón DIAZ RUBIO**

13 de septiembre de 2025

ESCUELA SUPERIOR DE LAS FUERZAS ARMADAS

PÁGINA INTENCIONADAMENTE EN BLANCO

EL PAPEL DE LA INTELIGENCIA EN LA GUERRA DE UCRANIA. ¿NUEVAS TECNOLOGÍAS Y NUEVOS PROCEDIMIENTOS?

Resumen

La guerra de Ucrania está marcando un antes y un después en el modo de empleo de las tecnologías, no solamente ceñido al campo de batalla, sino también en otros escenarios y dominios cuya contribución a aumentar el conocimiento situacional ha resultado ser imprescindible para el desarrollo de las operaciones.

El presente artículo explora cómo el empleo por Ucrania de diversos medios y sistemas tecnológicos, desde los drones que inundan los cielos hasta las redes sociales que conectan a millones de personas, pasando por los sistemas software de integración masiva de datos, ha llegado a proporcionarle una capacidad de obtención, recopilación y explotación de información en tiempo real y a una velocidad sin precedentes determinante para contrarrestar el poderío militar de Rusia y nivelar el resultado de la contienda.

Palabras clave

Guerra de Ucrania, medios ISR, obtención de información, tecnologías.

THE ROLE OF INTELLIGENCE IN THE UKRAINE WAR. NEW TECHNOLOGIES AND NEW PROCEDURES?

Abstract

The war in Ukraine is marking a turning point in the use of technology, not only on the battlefield but also in other scenarios and domains, whose contribution to increasing situational awareness has proven essential to the development of operations.

This article explores how Ukraine's use of various technological means and systems—from drones that fill the skies to social networks that connect millions of people, and massive data integration software systems—has given it the ability to gather, compile, and exploit information in real time and at an unprecedented speed, crucial to countering Russia's military power and leveling the outcome of the conflict.

Key words

War in Ukraine, ISR systems, collection information, technology.

Un vistazo previo al estallido de la guerra de Ucrania.

Antes de adentrarnos en el conflicto ruso-ucraniano a gran escala (febrero de 2022), conviene conocer en qué estado se encontraban las capacidades de obtención de información de Ucrania a través de un rápido análisis de los medios tecnológicos empleados en las actividades ISRⁱ en el conflicto del Donbás (2014-2021).

En el empleo de RPAS (Sistema de Aeronaves Pilotadas Remotamente), Ucrania carecía inicialmente de una fuerza propia. Durante este período cabe destacar el papel desempeñado por la población civil, donde organizaciones de naturaleza militar, como *Aerorozvidka*, surgieron para rellenar las carencias estatales, adaptando drones de uso comercial (COTS) para acometer misiones de reconocimiento de corto alcance y corrección de fuego de artillería en el campo de batalla¹.

Consciente de la dependencia externa, Ucrania impulsó su fuerza de RPAS a través de su industria de defensa con el desarrollo de drones autóctonos, como el *Leleka-100*, reforzada con la adquisición del *Bayraktar TB-2* (2021), hecho que marcó un salto cualitativo en las capacidades de reconocimiento y ataque de precisión a nivel operacional y estratégico².

El efecto producido por los UAVs (Vehículos Aéreos No Tripulados) empleados en el campo de batalla trajo consigo la eliminación de la sorpresa en las operaciones terrestres, la potenciación de la artillería, el aumento de las medidas de guerra electrónica y un gran impacto psicológico en las tropas. Los drones de bajo coste y fácil disponibilidad hicieron que el espacio aéreo fuera accesible para actores con recursos limitados (Ucrania), ofreciendo unas capacidades significativas en la obtención de información a nivel táctico.

Los sistemas satelitales de observación terrestre constituyen el principal activo de las actividades ISR a nivel estratégico, proporcionando una cobertura global, continua y no intrusiva. Durante el conflicto, Ucrania carecía de unas capacidades de observación espacial propias. Dependía pues de la inteligencia compartida por los socios occidentales (principalmente de EE.UU.) y de imágenes de satélites comerciales (*Maxar* y *Planet*) en fuentes abiertas por las que analistas ucranianos podían monitorizar a las unidades separatistas pro-rusas en la región del Donbás.

En 2014, ante la desinformación rusa, la sociedad ucraniana se movilizó empleando herramientas OSINTⁱⁱ para contrarrestar la narrativa del Kremlin y

ⁱ ISR (Inteligencia, Vigilancia y Reconocimiento). Actividades realizadas para la obtención de información, mayoritariamente por medios y sistemas como drones, satélites, sensores acústicos, cámaras, etc.

ⁱⁱ OSINT (Inteligencia de Fuentes Abiertas). Se refiere a la inteligencia derivada del proceso de obtención de información a partir de fuentes de acceso público y de carácter no clasificado, como medios de comunicación, publicaciones en redes sociales, etc.

documentar evidencias. Organizaciones no gubernamentales como *InformNapalm* geolocalizaban a soldados rusos en suelo ucraniano mediante fotografías de perfiles en redes sociales. Esta práctica evolucionó de un activismo social desordenado a un enfoque más sistemático, en el que el gobierno ucraniano combinó la inteligencia "subcontratada" que generaban los colectivos civiles con el desarrollo de capacidades estatales de obtención propias en fuentes abiertas³.

Para los meses inmediatamente anteriores a la invasión de 2022, el sistema OSINT ucraniano ya se había integrado en la estrategia de seguridad nacional, empleado de manera recurrente para proporcionar una alerta temprana. El análisis de imágenes satelitales comerciales y el seguimiento de actividades en redes sociales permitió a analistas independientes y estatales seguir la concentración de tropas rusas en la frontera ucraniana.

Evolución, no revolución.

Desde antes del estallido de la guerra (febrero de 2022), el gobierno de Ucrania ya había comenzado a adaptar sus fuerzas armadas al campo de batalla moderno, considerando la innovación y el desarrollo de medios y sistemas tecnológicos (incluidos los de obtención e intercambio de información) como uno de los principales ejes de la estrategia de defensa contra Rusia.

La necesidad de un conocimiento situacional multidominio (terrestre, marítimo, aeroespacial y del ciberespacio) promovió el desarrollo de las capacidades de obtención mediante una proliferación masiva de diversos medios ISR en todos los escenarios y niveles del conflicto (drones de reconocimiento y sensores a lo largo del campo de batalla, satélites de observación y herramientas de explotación permanente de fuentes abiertas), integrados en sistemas software de gestión del campo de batalla potenciados con inteligencia artificial (IA), capaces de procesar la información recopilada a una velocidad extraordinaria.

- Drones, los ojos del campo de batalla.

Ucrania ha demostrado una notable capacidad tecnológica para resistir y desafiar a Rusia mediante la adaptación y desarrollo de medios no tripulados, llegando a configurar un complejo sistema ISR que abarca desde sofisticados RPAS hasta enjambres de pequeños drones comerciales adaptados.

En el nivel operacional y estratégico, destacan los sistemas de altitud media y larga duración (MALE). El principal exponente es el *Bayraktar TB-2*, un RPAS de combate y de vigilancia/reconocimiento de hasta 27 horas de autonomía y un techo de servicio de 8.200 metros. Equipado con sensores electro-ópticos/infrarrojos (EO/IR) y capacidad de designación láser, realizó misiones ISR permanentes y de ataque con munición guiada. En las fases iniciales de la defensa de Kiev (febrero-marzo de 2022) desempeñó un papel destacado identificando puestos de mando y centros logísticos rusos que posteriormente

eran atacados. Sin embargo, su vulnerabilidad a las defensas antiaéreas y a la guerra electrónica más sofisticada redujo su uso en el frente a misiones esporádicas⁴.

En el nivel táctico, la adaptación masiva de drones comerciales (COTS) ha constituido la verdadera innovación tecnológica. El grueso de las misiones recayó en una amplia gama de RPAS tácticos, más pequeños, económicos y numerosos que actuaron como los "ojos" de las unidades de combate.

Por un lado, los UAVs tácticos de ala fija son los que ofrecen mayor autonomía y resistencia a la guerra electrónica que los de ala rotatoria. Entre ellos, el *Leleka-100* ucraniano, con una autonomía de 2,5 horas y 50 km de alcance, resistente a contramedidas electrónicas y equipado con sensores EO/IR, fue decisivo en la liberación de Jersón (noviembre de 2022), localizando depósitos de munición y puestos de mando en profundidad a la vez que efectuaba la evaluación de daños una vez que éstos eran atacados⁵.

El *SHARK UAS*, también de fabricación ucraniana, se empleó para penetrar hasta 60 km tras las líneas enemigas en el seguimiento de objetivos y actuar como relé de drones "kamikaze". El *RQ-20 Puma* de reconocimiento, con 3 horas de autonomía y 20 km de alcance, proporcionó un conocimiento situacional inmediato del terreno a nivel de sección y compañía. Ambos RPAS tuvieron un gran protagonismo durante la contraofensiva relámpago en la región de Járkov (septiembre de 2022) donde diseñaron un mapa detallado del despliegue defensivo ruso confirmando dónde se encontraban sus puntos más débiles⁶.

Por otro lado, los UAVs tácticos de ala rotatoria (cuadricópteros comerciales), como el *DJI Mavic 3*, representan la mayor revolución en el ámbito de empleo de drones durante el conflicto. De bajo coste (menos de 2.000 \$), fáciles de manejar, con cámaras de alta definición integradas, pero de autonomía limitada (40 minutos) y vulnerables a la guerra electrónica, han sido usados para reconocer, localizar y transmitir la posición de objetivos antes de ser atacados, además de guiar el fuego de artillería con precisión. En la defensa de Kiev, pequeños drones comerciales jugaron un papel vital en la localización de las columnas rusas, la identificación de objetivos de alto valor y el guiado del fuego de artillería, conformando un ciclo de "reconocimiento-ataque" altamente eficaz⁷.

Un claro ejemplo de la capacidad de adaptación e innovación ucraniana en este campo también lo podemos encontrar en los drones FPV (vista de primera persona). Se trata de un tipo de UAVs de carreras adaptados para portar cargas explosivas. Extremadamente rápidos (más de 150 km/h) y ágiles, permiten al operador identificar, seguir y apuntar al objetivo en tiempo real hasta el impacto, lo que provocó numerosas bajas y pérdidas materiales significativas entre las tropas rusas.

La ejecución de la ofensiva ucraniana en Kursk (agosto de 2024) fue posible gracias en parte a la neutralización de los sistemas de vigilancia de Rusia en la región. Las fuerzas ucranianas emplearon drones FPV contra UAVs de reconocimiento rusos, como el *Orlan*, permitiendo liberar temporalmente el



Imagen desde un dron FPV del ataque en la "Operación Telaraña" (*El Mundo*, 2025).

espacio aéreo, hecho clave para el desarrollo de las operaciones en el terreno⁸.

En la llamada "Operación Telaraña" en el interior de Rusia (junio de 2025), Ucrania combinó con éxito drones cuadricópteros FPV en la explotación de los "puntos ciegos" de la defensa aérea rusa y RPAS guiados por IA de manera autónoma para la detección y ataque de los aeródromos⁹.

Por lo tanto, puede afirmarse que el impacto general de los RPAS, gracias a esa vigilancia permanente del campo de batalla que otorga, ha ido desde la "caza" sistemática de la artillería rusa y el guiado de grupos de asalto de las unidades de combate, hasta la habilitación de ataques estratégicos sobre objetivos en territorio ruso.

- La omnipresente observación satelital.

La observación de la Tierra desde el espacio se sitúa en la cima de la pirámide ISR. Aunque Ucrania carecía de una constelación propia de satélites en 2022, ha adquirido una considerable suficiencia en la obtención y explotación de imágenes satelitales de alta calidad.

El modelo ucraniano se basa en una potente estrategia de acceso sustentada sobre tres pilares:

1º. La compartición de inteligencia de aliados occidentales, principalmente EE.UU. El suministro de informes provenientes de satélites de observación gubernamentales ha dotado a Ucrania de una notable capacidad estratégica de alerta temprana. Destacan satélites electro-ópticos de la serie *KeyHole-11* con una resolución inferior a 10 cm, satélites SAR (radar de apertura sintética) *Lacrosse/Onyx* de imágenes de alta resolución con visión nocturna y a través de nubes, y satélites SIGINTⁱⁱⁱ *Orion/Mentor*, que interceptan comunicaciones y detectan emisiones electromagnéticas en la superficie.

2º. Adquisición masiva y directa de información del sector espacial comercial o "New Space". Empresas como *Maxar* (EE.UU.), a través de sus satélites de la

ⁱⁱⁱ SIGINT (Inteligencia de señales). Inteligencia que proviene de la obtención y explotación de las señales y emisiones electromagnéticas.

serie *WorldView*, proporcionan imágenes multi y super-espectrales de hasta 30 cm de resolución, permitiendo identificar modelos de vehículos militares, evaluar daños e identificar posiciones defensivas. La compañía norteamericana *Planet*, que opera mediante la constelación *PlanetScope* (más de 200 minisatélites que escanean diariamente la Tierra con una resolución de 3 metros) y *SkySat* (21 satélites con 50-70 cm de resolución), permite obtener imágenes muy detalladas varias veces al día sobre una misma área, ideal para el seguimiento de unidades. *ICEYE* (Finlandia) posee una constelación de 44 satélites SAR que operan bajo cualquier condición meteorológica, proporcionando también una observación "todo tiempo" de zonas de interés.

3º. Un esfuerzo por desarrollar capacidades soberanas. Aunque la dependencia externa es excesivamente acusada, Ucrania aspira a tener sus propios sistemas espaciales. El *Sich-2-30* (lanzado en enero de 2022) es un satélite óptico con una resolución de 7,8 metros, pero su aportación ha sido marginal debido a continuos problemas operativos desde el primer momento.

La información satelital ha sido un multiplicador importante para Ucrania, dotándole de un amplio conocimiento situacional y una altísima precisión en la selección de objetivos. Durante la defensa de Kiev fue fundamental para identificar, rastrear y atacar la columna rusa de más de 60 km estancada al norte de la capital. Imágenes continuas de satélites comerciales como *Maxar* mostraron al mando ucraniano la magnitud y composición de dicha columna, permitiendo la ejecución de ataques de artillería y de unidades motorizadas sobre sus puntos más débiles, contribuyendo así al fracaso del asalto inicial ruso¹⁰.

GEOINT^{iv} jugó un papel decisivo en la campaña del Mar Negro y península de Crimea. El modelo de "flota fantasma" ucraniana, basado en la capacidad de detectar un objetivo con un satélite, rastrearlo con un dron aéreo, confirmar su identidad con un USV (dron de superficie naval) y atacarlo con diferentes sistemas (USVs y misiles), convirtió el Mar Negro en una zona de acceso prohibido para la armada rusa. Destacan las operaciones de hundimiento del crucero *Moskva* (abril de 2022) y de los ataques al astillero de Sebastopol y al edificio del cuartel general de la Flota (septiembre de 2023), las cuales requirieron una localización precisa que sólo las imágenes de los satélites fueron capaces de proporcionar¹¹.

La liberación de Jersón (noviembre de 2022) es un ejemplo de campaña de desgaste logístico habilitada por la observación satelital. La sincronización de sistemas de artillería *HIMARS* con información geoespacial permitió identificar, georreferenciar y atacar objetivos de alto valor como puentes, depósitos de

^{iv} GEOINT (Inteligencia geoespacial). Derivada de la explotación y análisis de información geoespacial procedente de imágenes, mapas y datos GPS para describir, evaluar y representar las características físicas y actividades georreferenciadas de la superficie terrestre.

munición y puestos de mando, aislando a las unidades rusas y forzando su retirada.

En la fase de “guerra de desgaste y ataques estratégicos” (2023-2025), la información satelital fue aún más crucial. Durante la contraofensiva ucraniana de verano de 2023, a través de GEOINT se monitorizó los cambios en las fortificaciones defensivas rusas y se evaluó la eficacia de los ataques de artillería.

Asimismo, la campaña de ataques con drones de largo alcance contra refinerías de petróleo y bases aéreas en territorio ruso a partir de 2024 se basó en la información satelital para la selección de objetivos y verificación del alcance de los daños en las instalaciones¹².



Imagen satélite (*Maxar*) de un depósito de munición en Toropets, Rusia (*TIME*, 2025).



Imagen satélite (*Maxar*) del mismo depósito tras ser atacado con UCAVs (*TIME*, 2025).

¿Y qué hay de los satélites *Starlink* de la compañía *SpaceX*, propiedad del multimillonario Elon Musk? Pues bien, es imprescindible señalar que la constelación satelital *Starlink* no se dedica a la observación de la Tierra. Su impacto, eso sí, trascendental en el desarrollo del conflicto, no reside en la capacidad para observar el campo de batalla, sino en su función habilitadora por la cual se conectan todos los medios y sistemas ISR ucranianos. Actualmente existen alrededor de 60.000 terminales *Starlink* de uso civil y militar en toda Ucrania, lo que le convierte en una infraestructura crítica para la defensa.

- OSINT y la guerra digital en abierto.

Puede decirse que el conflicto de Ucrania es el primero documentado por ciudadanos conectados globalmente en tiempo real. La inteligencia de fuentes abiertas ha sido imprescindible para explotar esa avalancha de datos generados en Internet, desde publicaciones en redes sociales hasta imágenes satelitales comerciales, poniendo a disposición de los mandos ucranianos una información valiosa que sería utilizada en la confección de las operaciones.

La principal fuente OSINT la conforman las redes sociales y plataformas de mensajería online. De entre todas, la aplicación rusa *Telegram* supone el epicentro informativo para ambos bandos, permitiendo a los analistas ucranianos

monitorizar sus canales para geolocalizar unidades, seguir el movimiento de convoyes logísticos y obtener información sobre el estado y moral de las tropas enemigas a través de vídeos e imágenes publicados. La también aplicación de origen ruso *Vkontakte* (principal red social en Rusia con el 90% usuarios de Internet) ha sido una fuente importante de información sobre perfiles y grupos para los investigadores en la identificación del historial de soldados, localización de sus unidades e incluso familiares.

La red social *Twitter/X* constituye el principal foro de análisis y publicaciones de la comunidad OSINT mundial, donde analistas de *GeoConfirmed* y *Bellingcat* (organizaciones de voluntarios dedicadas a la geolocalización y verificación de contenido visual en zonas de conflicto) publican información sobre la ubicación de las tropas rusas, originando un proceso de revisión por pares en tiempo real. Otra aplicación de ámbito mundial utilizada en la guerra ha sido *TikTok*, especialmente en los primeros meses. Su algoritmo viral basado en vídeos de corta duración ha permitido obtener un conocimiento tanto de las unidades en el terreno como de numerosos ataques que no aparecían en otras aplicaciones.

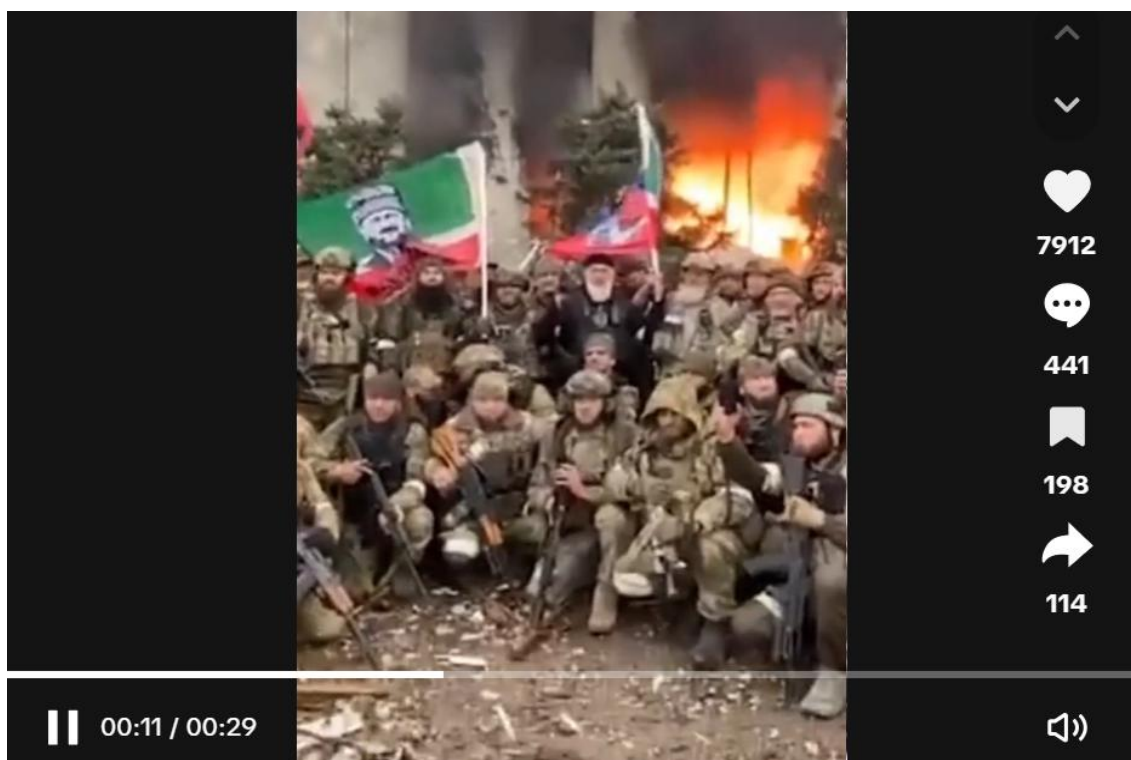


Imagen que muestra el estado de las tropas chechenas tras la toma de Mariupol en un video publicado en la aplicación *TikTok* (*El Mundo*, 2022).

La institucionalización de OSINT es una de las señas de identidad del conflicto. El gobierno ucraniano creó mecanismos formales para canalizar el potencial de las fuentes abiertas y la información ciudadana hacia su aparato de defensa. La plataforma *eVorog* (canal de *Telegram* operado por el Ministerio de Transformación Digital) permitió a millones de personas informar de forma anónima sobre la ubicación y movimiento de unidades rusas mediante fotos y

videos geolocalizados. Este sistema creó un flujo masivo de datos que, una vez verificados y procesados, se entregaba a las unidades en el terreno, construyendo una imagen en tiempo real del campo de batalla a la par que iba alimentando directamente el ciclo de inteligencia táctica¹³.

Además de las redes sociales y aplicaciones de mensajería instantánea, a través de fuentes abiertas se han empleado numerosas herramientas verdaderamente útiles en la contextualización y verificación de la información de la guerra.

Entre ellas caben mencionar las de: geolocalización, como *Google Earth Pro*, *Google Street View* (para comparar videos con imágenes a nivel de calle) y *Yandex Maps* (que ofrece imágenes satélite más actualizadas de zonas de Rusia y territorios ocupados); de cronolocalización y verificación, empleadas para la detección de campañas de desinformación (*SunCalc.net*, *Google Images*, *TinEye* y *Yandex Images*); de monitorización, por medio de mapas interactivos como *DeepStateMap.live* y *ArcGIS*, y de herramientas de rastreo de tráfico aéreo (*Flightradar24*, *ADS-B Exchange*) y marítimo (*MarineTraffic*, *VesselFinder*).

La contribución de OSINT a las operaciones durante la guerra ha sido destacada, ayudando a clarificar la "niebla de guerra" en distintos escenarios. Los días previos al estallido, la información obtenida en fuentes abiertas desacreditó la narrativa rusa y confirmó la acumulación de tropas en la frontera. Una vez iniciada la invasión, las fotos y vídeos publicados en redes sociales por soldados rusos eran geolocalizados por analistas y la información extraída se difundía a las unidades desplegadas¹⁴. Ya en la fase de ataques sobre objetivos de interés en territorio de Rusia, los analistas verificaban el alcance de los daños mediante videos de explosiones e imágenes satelitales comerciales en fuentes abiertas.

- Los sistemas de gestión del campo de batalla.

Uno de los aspectos más interesantes, en términos de desarrollo tecnológico, tiene que ver con el modo en que las Fuerzas Armadas de Ucrania (AFU), su Ministerio de Transformación Digital y determinados grupos de voluntarios han aunado fuerzas y afrontado la necesidad de diseñar e implementar sistemas de gestión del campo de batalla (BMS por sus siglas en inglés) con unos recursos muy limitados, demostrando una notable capacidad de adaptación, incluso desde antes de la invasión de febrero de 2022.

Actualmente, un militar ucraniano puede tener acceso a una decena de programas y aplicaciones autóctonas como *Kropyva*, *MilChat*, *DELTA*, *GisArta*, *Terminal*, *ComBat Visión*, *Virazh Planshet*, entre otras. Dos de ellas están consideradas como pilares fundamentales para la gestión del campo de batalla: *Kropyva* y *DELTA*.

La aplicación de estos sistemas desde 2022 ha reducido el ciclo OODA (Observar, Orientar, Decidir, Actuar) a menos de un minuto, y ha mejorado

drásticamente la conciencia situacional en todos los niveles de mando, convirtiéndose en un factor determinante en el campo de batalla.



Software del BMS *Kropyva* (*ArmySOS*)

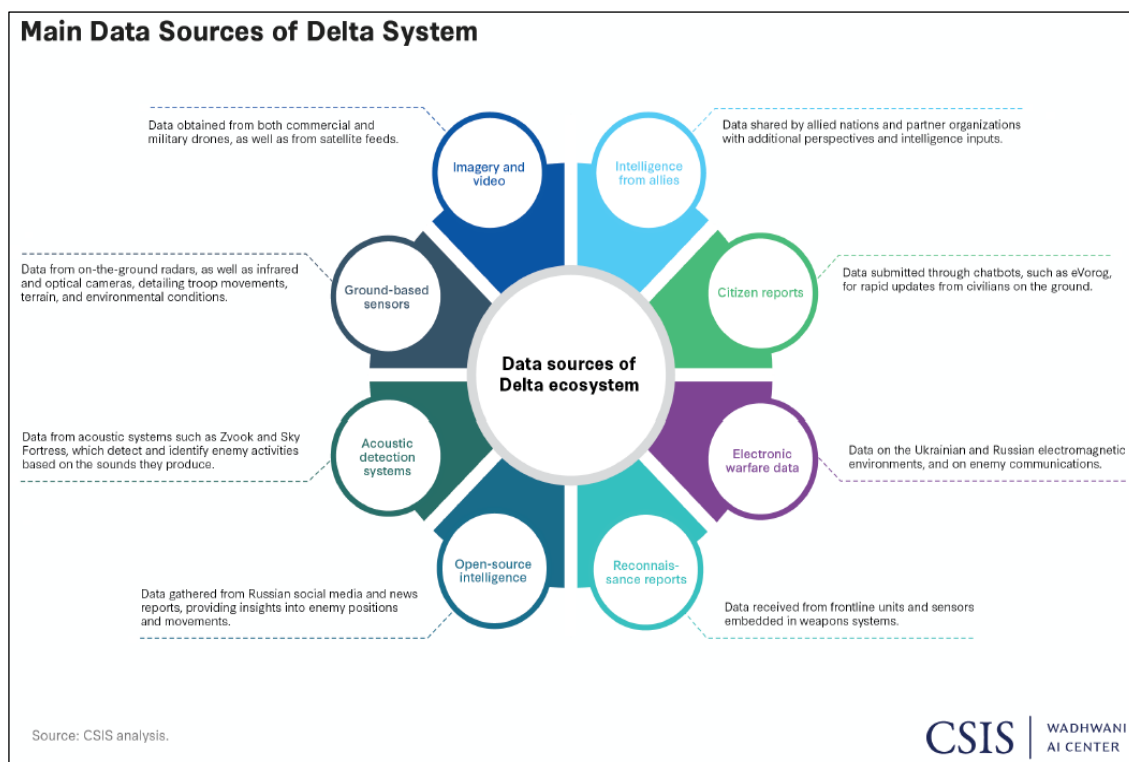
Kropyva (“ortiga”) surgió en 2014 a manos de una organización voluntaria no gubernamental para solventar la falta de mapas actualizados y compartir información de manera rápida. Con el paso de los años ha evolucionado de una herramienta de geolocalización en tablets a un potente software, de uso generalizado en cientos de unidades ucranianas con más de 200.000 terminales.

Los UAVs conforman el principal medio de obtención de *Kropyva*, permitiendo a los operadores fijar y difundir las coordenadas de los objetivos localizados directamente en la aplicación. Desempeña un rol crucial al permitir la recopilación, procesamiento y difusión de información táctica en tiempo real, convirtiendo a cada combatiente y medio ISR en nodos de una extensa red de obtención¹⁵.

Si *Kropyva* representa la digitalización a nivel táctico, *DELTA* constituye el cerebro y el sistema nervioso central del esfuerzo bélico informatizado de Ucrania. Creada en 2016 por el grupo de ingenieros voluntarios *Aerorozvidka*, su principal función en inteligencia es agregar, fusionar y visualizar datos de una inmensa variedad de fuentes para crear una imagen común, unificada y en tiempo real del entorno, dando cobertura a casi todas las AFU y proporcionando a los mandos un amplio conocimiento situacional. Desde 2023 es administrada por el Centro de Innovación y Desarrollo de Tecnología de Defensa del Ministerio de Defensa de Ucrania.

El sistema *DELTA* es empleado en todas las ramas y niveles del ejército ucraniano, disponible tanto para los escalones básicos a través de dispositivos móviles (teléfonos y tablets), como para los órganos de mando. Opera a modo de un sistema basado en la “nube” donde la información obtenida es tratada por varios centros de conciencia situacional, localizados en ocho ciudades a lo largo de todo el frente, que recopilan y fusionan datos en tiempo real del campo de batalla procedentes de una amplia variedad de medios como drones, satélites, cámaras, radares, unidades de reconocimiento e incluso de aplicaciones de mensajería online integradas (*eVorog*)¹⁶.

Una novedad destacable de *DELTA* es su constante evolución y adaptación a los estándares OTAN que garantizan la interoperabilidad del sistema con plataformas aliadas de cara a futuras operaciones conjuntas. En 2023, *DELTA* demostró ser compatible con quince sistemas análogos de diferentes países, incluyendo tres desarrollados por la OTAN. Su interoperabilidad fue probada con éxito en el “NATO CWIX-24” en julio de 2024, evidenciando su capacidad para fusionar información ISR de diversos dominios y contribución a un conocimiento situacional integral del campo de batalla.



Fuentes de datos del sistema *DELTA* (CSIS, 2024).

En cuanto al desarrollo de las operaciones, *DELTA* ha funcionado como sistema nervioso digital de las fuerzas ucranianas, proporcionando una superioridad en la información decisiva, acelerando el ciclo "sensor-tirador" y actuando como un capacitador clave en los triunfos más significativos de la guerra.

Durante los primeros días de la invasión, *DELTA* fue la herramienta que permitió a los defensores ucranianos establecer un orden a partir del caos inicial, integrando información de puestos de observación, transmisiones de vídeo de pequeños drones comerciales y avisos de los ciudadanos sobre los movimientos del enemigo. Esta capacidad para recopilar y fusionar información táctica en tiempo real y distribuirla a las unidades en el frente fue fundamental para la defensa móvil que frenó el avance ruso sobre Kiev¹⁷.

En las operaciones de largo alcance contra objetivos en Crimea en septiembre de 2023, y desde 2024 en Rusia (refinerías y bases aéreas), *DELTA* actuó como plataforma de fusión de información estratégica en la integración de datos de

satélites y de fuentes OSINT para construir una imagen detallada de los objetivos de alto valor y sus defensas. Esto contribuyó a una planificación de misiones complejas con el empleo de misiles y drones de largo alcance al disponer de una información actualizada¹⁸.

- El papel multiplicador de la inteligencia artificial.

En los últimos años, las fuerzas ucranianas han utilizado la IA como un multiplicador de las capacidades de recopilación y procesamiento de información mediante la explotación masiva de fuentes abiertas y la fusión de datos geoespaciales y de vídeos e imágenes de drones. Actualmente, su uso por Ucrania continúa supeditado al control humano, quien en última instancia toma las decisiones en función de los análisis proporcionados por la IA, previamente supervisados.

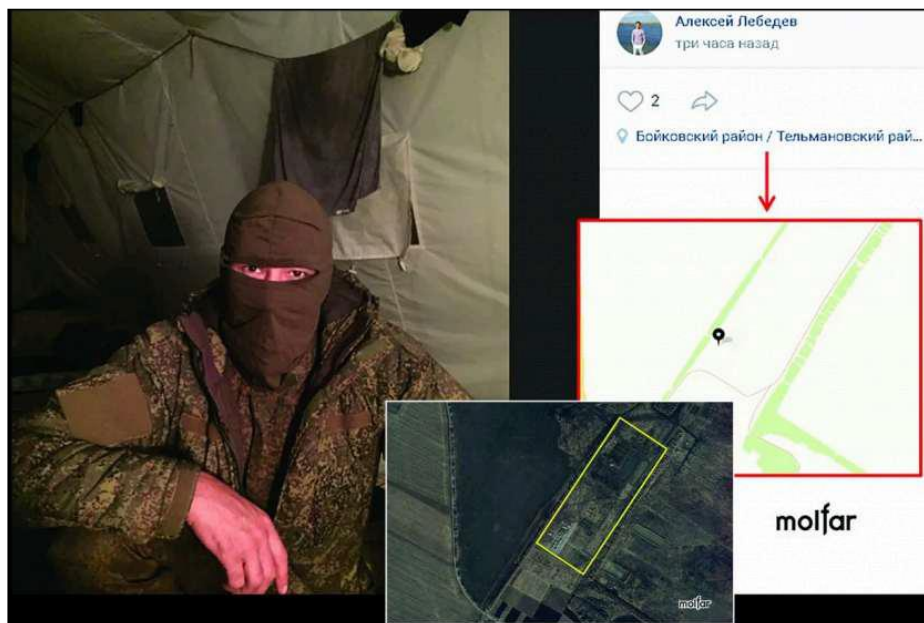
Una de las aplicaciones más destacadas de la IA es la fusión y análisis de datos en tiempo real. La participación de empresas tecnológicas aliadas, como la estadounidense *Palantir* desde verano de 2022, ha sido vital. Especializada en el análisis asistido por IA de Big Data, su software *Gotham* integra datos de diferentes fuentes, desde imágenes de satélites comerciales hasta información clasificada del gobierno y de los aliados, proporcionando a los altos mandos ucranianos un mejor conocimiento situacional y control de las operaciones¹⁹.

La imprescindible aportación de empresas tecnológicas occidentales en IA se ha complementado en los últimos años con el desarrollo y aplicación de sistemas ucranianos. Ingenieros locales han desarrollado plataformas como *OCHI*, que centraliza retransmisiones de video de miles de UAVs, mientras que la empresa de IA *Griselda* procesa datos de satélites, UAVs y de redes sociales en tiempo real, almacenando y difundiendo automáticamente la información a los organismos correspondientes (entre ellos *DELTA*) en menos de 30 segundos²⁰.

Los algoritmos de IA desarrollados por estas plataformas han permitido a las fuerzas ucranianas analizar ingentes cantidades de datos, especialmente útiles para: la detección y reconocimiento de equipamiento militar ruso; el análisis de patrones de actividad mediante el rastreo del movimiento de unidades, y la selección de objetivos con el cálculo del grado de efectividad en los ataques para su ejecución por medio de drones o fuego de artillería.

En el campo de OSINT, la IA ha desempeñado un papel fundamental en la recopilación y análisis automatizado de contenidos.

Para la identificación y geolocalización, el sistema *ODCR Assistant* utiliza IA para monitorizar y analizar redes sociales rusas, consiguiendo rastrear posiciones y movimientos de las unidades. Mediante el filtrado de publicaciones, es capaz de reconocer los indicadores clave y estructurar la información recopilada que posteriormente es entregada a los analistas. La empresa ucraniana *Molfar* también emplea IA para vincular información extraída de *Telegram* y *Vkontakte* en la geolocalización de personas de interés.



Geolocalización extraída por *Molfar* de la publicación de un soldado ruso en *Vkontakte* tras haberse conectado con su smartphone (Revista *Ejércitos*, 2023).

Una de las aplicaciones más notorias ha sido el software de reconocimiento facial de la compañía norteamericana *Clearview AI*, que cuenta con una base de datos de decenas de miles de millones de imágenes, y es utilizado por el Ministerio de Defensa ucraniano para identificar fotos en redes sociales de soldados enemigos fallecidos, verificar identidades en puntos de control y reconocer a individuos implicados en posibles crímenes de guerra²¹.

En la lucha contra la desinformación, plataformas como *Mantis Analytics* y *Osavul* (ambas ucranianas) se valen de la IA para recopilar información de redes sociales y medios de comunicación en tiempo real, detectando campañas de desinformación y narrativas prorrusas e identificando bots difusores de propaganda enemiga.

La IA también ha mejorado las capacidades SIGINT, habilitando el desarrollo de software de reconocimiento por voz y traducción basado en IA para monitorizar comunicaciones no encriptadas. La empresa estadounidense *Primer* ha acelerado el proceso de transcripción de las llamadas interceptadas de soldados rusos en el frente²².

Otra de las aplicaciones de la IA la podemos encontrar en el despliegue de sistemas de detección acústica como esfuerzo complementario a la capacidad de detección de ataques aéreos rusos. Destaca el sistema *Zvook*, red de sensores acústicos instalados en puntos cercanos a la frontera con Rusia que utiliza el aprendizaje automático para detectar helicópteros, drones, aviones de combate y misiles de crucero a baja cota, proporcionando alerta temprana a los sistemas de defensa antiaéreos.

En cuanto a los UAVs, la IA se ha convertido en una herramienta fundamental para el almacenamiento y procesamiento de datos. Si bien la implementación definitiva de la IA en drones ISR para funciones plenamente autónomas aún está en desarrollo, modelos evolucionados como el *SmartPilot* ya incorporan IA para buscar, identificar y atacar objetivos por sí solos.

El *Saker Scout*, un dron de IA basado en aprendizaje automático, puede detectar, identificar y atacar hasta 64 tipos de objetos militares. Su software permite reconocer y obtener información de manera autónoma de un área, proporcionando detalles sobre posiciones defensivas y el despliegue de unidades en apenas unos minutos²³.

Mirando hacia el futuro.

Si bien para antes de 2022 Ucrania ya había comenzado a desarrollar sus capacidades ISR, la invasión rusa a gran escala aceleró el ritmo de innovación tecnológica, impulsando una rápida y profunda adaptación de los medios existentes para su empleo en todo el espectro del conflicto. El inmenso flujo de datos generado propició la integración de esos medios ISR en sistemas de gestión del campo de batalla, permitiendo a las fuerzas ucranianas obtener una mejor conciencia situacional que se tradujo en una toma de decisiones más rápida, precisa y coordinada.

Al igual que en otros conflictos armados del pasado, la guerra de Ucrania ha servido como laboratorio de pruebas, en este caso en lo relativo al desarrollo e implementación de las tecnologías y la capacidad de adaptarla a las necesidades de inteligencia según las circunstancias. La guerra de la superioridad de la información, convertida en un factor decisivo para cualquier contienda, está en marcha, y sus lecciones pueden marcar un punto de inflexión en la preparación de los conflictos de la era moderna.

Pedro Ramón Díaz Rubio

Bibliografía

- ¹ Kofman, M. y Rojansky, M. (2015) "A closer look at Russia's hybrid war in Ukraine". *Kennan Institute*, núm. 7, abril.
- ² Çetiner, Y. (2021) "Los vehículos aéreos no tripulados modelo Leleka-100 se agregan al inventario del ejército ucraniano". *Overt Defense*, 25 de mayo.
- ³ Giles, K. (2016) "Las nuevas herramientas de Rusia para enfrentar a Occidente: continuidad e innovación en el ejercicio del poder de Moscú". *Chatham House*, 21 de marzo.
- ⁴ Marcelin, J. y Khomenko, I. (2025) "El Bayraktar TB2 ucraniano vuelve al combate: ¿por qué ahora y dónde ha estado? La historia completa de una leyenda de guerra". *UNITED24 Media*, 26 de junio.
- ⁵ Hird, K. et al. (2022) "Russian Offensive Campaign Assessment". *Institute for the Study of War & AEI's Critical Threats Project*, 18 de octubre.
- ⁶ Khurshudyan, I., Ilyushina, M. y Khudov, K. (2022) "Rusia y Ucrania están librando la primera guerra de drones a gran escala". *Washington Post*, 2 de diciembre.
- ⁷ Moyano, F.J. (2023) "La guerra en Ucrania y las batallas en zona urbana". *Revista Ejércitos*, 20 de diciembre.
- ⁸ Boyer, D. y Becker, R. (2024) "How Ukraine overcame the transparent battlefield to achieve operational surprise in Kursk". *TRADOC G2*, 19 de septiembre.
- ⁹ Serbin, A. (2025) "Telaraña letal: el golpe de drones ucranianos que derriba la ilusión de una retaguardia segura en Rusia". *Infobae*, 2 de junio.
- ¹⁰ Johnson, J. (2022) "Cómo Maxar está ayudando a vencer a los rusos con sus cuatro ojos en el cielo". *The Telegraph*, 8 de junio.
- ¹¹ Rishko, V. (2024) "Socavar el dominio naval de Rusia: la campaña estratégica de Ucrania en el Mar Negro y Crimea". *Transatlantic Dialogue Center*, 23 de agosto.
- ¹² Díaz, J. (2025) "Satélites detectan que Ucrania ha vaporizado las armas de una base de bombarderos nucleares rusos". *El Confidencial*, 25 de marzo.
- ¹³ Rosado, S.G. (2023) "La inteligencia de fuentes abiertas (OSINT) en la guerra de Ucrania". *Revista Ejércitos*, 24 de julio.

¹⁴ Hewson, J. (2023) "La empresa ucraniana que utiliza las redes sociales y la tecnología de fuentes abiertas para contrarrestar la invasión rusa". *PBS News*, 19 de abril.

¹⁵ MacAlpine, A. (2024) "El arma secreta de Ucrania, el software 'Kropyva'". *UNITED24 Media*, 29 de noviembre.

¹⁶ Soesanto, S. (2024) "La manera de guerra digital ucraniana. Voluntarios, aplicaciones y plataformas de intercambio de inteligencia". *Center for Security Studies*.

¹⁷ Collins, L. y Spencer, J. (2025) "Urban Warfare Project Case Study 12: Battle of Kyiv". *Modern War Institute*, 21 de febrero.

¹⁸ Bondar, K. (2024) "¿Tiene ya Ucrania tecnología CJADC2 funcional? *Center for Strategic & International Studies*, 11 de diciembre.

¹⁹ Bergengruen, V. (2024) "Cómo los gigantes tecnológicos convirtieron a Ucrania en un laboratorio de guerra de IA". *TIME*, 8 de febrero.

²⁰ Tregub, C. (2024) "La frontera de la IA: el papel de Ucrania en el futuro de la guerra". *Friends of Europe*, 13 de octubre.

²¹ Hill, K. (2022) "El reconocimiento facial va a la guerra". *The New York Times*, 7 de abril.

²² Fontes, R. y Kamminga, J. (2023) "Ucrania: un laboratorio viviente para la guerra de IA". *National Defense Magazine*, 24 de marzo.

²³ Hambling, D. (2023) "Los drones de IA ucranianos buscan y atacan a las fuerzas rusas sin la supervisión humana". *Forbes*, 17 de octubre.