



Artículo de Investigación

## LA MUERTE DESDE ARRIBA: EMPLEO DE DRONES DE ATAQUE POR ORGANIZACIONES TERRORISTAS

Diego de Lorenzo de Guindos  
Alférez de la Guardia Civil  
Cursando Grado en Ingeniería de la Seguridad  
[delorenzodeguindos@gmail.com](mailto:delorenzodeguindos@gmail.com)

Recibido 07/09/2025  
Aceptado 19/11/2025  
Publicado 30/01/2026

doi: <https://doi.org/10.64217/logosguardiacivil.v4i1.8472>

Cita recomendada: de Lorenzo, D. (2026). La muerte desde arriba: empleo de drones de ataque por organizaciones terroristas. *Revista Logos Guardia Civil*, 4 (1), 53–82. <https://doi.org/10.64217/logosguardiacivil.v4i1.8472>

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)

Depósito Legal: M-3619-2023

NIPO en línea: 126-23-019-8

ISSN en línea: 2952-394X



## LA MUERTE DESDE ARRIBA: EMPLEO DE DRONES DE ATAQUE POR ORGANIZACIONES TERRORISTAS

**Sumario:** 1. INTRODUCCIÓN. 2. DRONES DE ATAQUE EN GUERRAS CONVENCIONALES. 2.1. Guerra Civil Siria. 2.2. Guerra de Ucrania. 3. OPERACIÓN TELARAÑA. 3.1. El ataque del 1 de junio de 2025. 3.2. La operación. 3.3 Diferencias con otras operaciones similares. 3.4. Consecuencias. 4. LOS DRONES DE ATAQUE LLEGAN A SUDAMÉRICA. 4.1 México. 4.2 Colombia. 4.3 SOLUCIONES PROPUESTAS. 5. APLICACIÓN DE LAS LECCIONES. 5.1 Lecciones aprendidas en anteriores atentados. 5.2. Posibilidades de atentados terroristas con drones. 5.3. Atacar la línea de suministro. 5.4. Fases delicadas del proceso de preparación de un atentado con UAS. 6. CONCLUSIONES. 7. REFERENCIAS BIBLIOGRÁFICAS. 8. NORMATIVA.

**Resumen:** Los drones de pequeñas dimensiones se han convertido en sistemas cada vez más presentes en los escenarios de conflicto. Su versatilidad, amplia disponibilidad y bajo coste explican esta expansión. Este artículo analiza la posibilidad de que estos dispositivos puedan incorporarse a tentativas de atentados terroristas, examinando previamente los usos que han recibido en conflictos bélicos, con especial atención a las acciones en la retaguardia, cuya naturaleza podría resultar inspiradora para la planificación de ataques. Con el fin de valorar la utilidad operativa de los drones para actores con capacidades logísticas, económicas y operativas inferiores a las de los Estados, se estudiará también su empleo por parte de organizaciones criminales en Sudamérica. Las conclusiones obtenidas se pondrán en relación con las vulnerabilidades históricamente explotadas por grupos terroristas para evadir la acción del Estado y materializar sus operaciones. El artículo concluye que los drones constituyen herramientas especialmente atractivas para estos grupos, y que su proliferación implica la aparición de nuevas vulnerabilidades que deberán ser identificadas y corregidas para prevenir atentados contra el Estado o sus ciudadanos.

**Abstract:** Small drones have become increasingly present in conflict scenarios. Their versatility, wide availability, and low cost explain this trend. This article examines the possibility that such devices may be incorporated into attempted terrorist attacks, first analyzing their use in armed conflicts, with particular attention to rear-area operations, whose characteristics could inspire the planning of attacks. To assess the operational utility of drones for actors with more limited logistical, economic, and operational capabilities than states, the article also explores their use by criminal organizations in South America. The findings are then related to the vulnerabilities historically exploited by terrorist groups to evade state action and carry out their operations. The article concludes that drones constitute highly attractive tools for these groups and that their proliferation entails the emergence of new vulnerabilities that must be identified and addressed to prevent potential attacks against the state or its citizens.

**Palabras clave:** Drones, Inteligencia Artificial, Terrorismo, Ucrania, Atentados.

**Keywords:** Drones, Artificial Intelligence, Terrorism, Ukraine, Terrorist Attacks

## ABREVIATURAS

11-S: Atentados del 11 de septiembre

CDS: Cártel de Sinaloa

CIA: Agencia Central de Inteligencia

CJNG: Cártel de Jalisco Nueva Generación

DEA: Administración de Control de Drogas de los EE. UU.

EIIL/EI: Estado Islámico en Irak y el Levante

EE. UU.: Estados Unidos

FARC: Fuerzas Armadas Revolucionarias de Colombia

FBI: Buró federal de Investigaciones

FPV: First Person View

GPS: Sistema de Posicionamiento Global

IA: Inteligencia Artificial

OCT: Organizaciones Criminales Transnacionales

RPAS: Sistema de Aeronaves Pilotadas Remotamente

SBU: Servicio de Seguridad de Ucrania

UAS: Unmanned Aerial Systems

UAV: Unmanned Aerial Vehicles

## 1. INTRODUCCIÓN

El ser humano siempre ha hecho uso de los avances en la ciencia para aumentar su capacidad militar. En algunos casos, ha adaptado los descubrimientos existentes a fines bélicos; en otros, ha sido precisamente la necesidad de obtener medios de destrucción más potentes y eficaces que los de sus adversarios la que ha impulsado auténticas revoluciones tecnológicas.

En una de esas etapas de conflicto se desencadenó una explosión científica sin precedentes en todas las ramas: la Segunda Guerra Mundial. De todos los proyectos, grandes ideas y descubrimientos, nos gustaría detenernos particularmente en dos de ellos para analizar sus consecuencias a largo plazo: los proyectos alemanes que llevaron al empleo de los misiles balísticos V1 y V2, así como el “Proyecto Paloma”.

En primer lugar, los proyectos alemanes que llevaron al empleo de los misiles balísticos V1 y V2. Podían ser lanzados desde el territorio de la Francia ocupada y alcanzar ciudades en Inglaterra, en las que causaron auténticos estragos (Reuter, 2000).

En segundo lugar, un proyecto más desconocido, aunque no por ello menos revolucionario, fue el “Proyecto Paloma” del psicólogo americano B.F. Skinner para desarrollar misiles antibuque guiados mediante tecnología IA (aunque en este caso, IA significaría “inteligencia animal”). Basándose en las conclusiones del Perro de Pavlov, Skinner concluyó que las palomas podrían ser entrenadas para picar continuamente en un punto que viesen en una pantalla. Ese punto en algún momento habría sido un buque enemigo real, y los puntos en los que la paloma picaba enviarían señales a los controles del misil para modificar su trayectoria. El proyecto se suspendió en 1953 por el avance de las medidas de guiado electrónico (Skinner, 1960).

Aunque estos dos proyectos guardan poca relación directa con el desarrollo de los drones, fueron los primeros en implantar ideas que hoy en día son una realidad. El primero propuso poder atacar objetivos enemigos a una gran distancia con misiles que no pusieran en riesgo la vida de ningún piloto, y el segundo fue el primer paso hacia sistemas de armas que pensarán por sí mismos y tomarán sus propias decisiones, sin necesidad de intervención humana y sin emitir radiación electromagnética para detectar los objetivos, pues las palomas lo hacían con una interpretación de imágenes. Estos experimentos sentaron las bases conceptuales para la automatización de armas, una idea que décadas después evolucionaría hacia los actuales drones de combate.

En la actualidad, a fecha de septiembre de 2025, no tenemos palomas que guíen proyectiles planeadores lanzados desde aviones. En su lugar, tenemos pequeños aparatos voladores cargados de explosivos con la capacidad de entender dónde están, hacia dónde deben ir, cuál es su misión y reconocer los potenciales objetivos para decidir cuál es el más adecuado y estrellarse contra él, detonando los explosivos en el proceso.

Este fenómeno ha pasado a considerarse parte habitual del panorama bélico contemporáneo, pero tal vez con una delimitación espacial excesivamente confiada: es un fenómeno propio de las líneas del frente de las guerras. Sin embargo, las continuas acciones ucranianas y rusas a retaguardia con drones a cientos de kilómetros del frente, y las noticias que nos llegan desde Sudamérica en lo relativo a su uso por grupos de

delincuencia organizada nos hacen sospechar de los posibles usos que grupos terroristas le podrían dar a estos aparatos.

El objetivo del presente artículo es analizar, en primer lugar, el potencial de los medios aéreos no tripulados para ser empleados en ataques dirigidos contra objetivos militares, así como ejemplos históricos recientes de esta utilización. Posteriormente, se procederá a explorar la transposición de estos sistemas a organizaciones que operan al margen del Estado que se ha sucedido en países de Sudamérica, principalmente México, Colombia y Brasil. A continuación, se tomarán atentados terroristas pasados para resaltar los errores cometidos que posibilitaron la comisión de estos. Todos los apartados anteriores sustentarán la tesis final, que es la de que los drones son un sistema especialmente atractivo para aquellos que traten de realizar ataques contra grandes masas de personas, así como objetivos concretos.

De cara a este artículo, se adoptará como definición de terrorismo la contenida en una directiva del Departamento de Defensa de los EE. UU.: “uso calculado de la violencia o de la amenaza de violencia contra individuos o propiedades, para infundir miedo, con la intención de coaccionar o intimidar al gobierno o a sociedades para conseguir objetivos políticos, ideológicos o religiosos” (*Department of Defense*, 2000). No obstante, se considerarán de forma analógica las acciones que se manifiesten a través de las mismas conductas externas, aunque no persigan una finalidad política, ideológica o religiosa.

Con la finalidad de acotar el ámbito de este artículo, se obviará el empleo de drones de grandes dimensiones. Esto es en consideración de su escasa disponibilidad y su mayor facilidad de detección. Quedan por tanto excluidos de este estudio los drones empleados por la Fuerza Aérea de los Estados Unidos, los pertenecientes a las fuerzas ucranianas y rusas, así como cualquier otro de idéntica consideración.

Queda por tanto definido como objeto de estudio el empleo de drones de pequeñas dimensiones por grupos que persigan acciones violentas contra grupos de personas, altas personalidades, propiedades importantes para la sociedad, y el resto de las que entren dentro de la definición de atentado.

## **2. DRONES DE ATAQUE EN GUERRAS CONVENCIONALES**

### **2.1. GUERRA CIVIL SIRIA**

El papel de los drones de pequeñas dimensiones en conflictos ha vivido un aumento progresivo hacia lo que hoy conocemos. Los primeros usos de entidad considerable pudieron ser detectados durante la guerra civil siria, donde más concretamente, el Estado Islámico en Irak y el Levante (EIIL/EI) exploró las posibilidades ofensivas de los Vehículos Aéreos No Tripulados (UAV) (Hambling, 2016).

En este contexto, el primer uso registrado de empleo de drones como herramientas de ataque fueron las combinaciones dron-coche bomba con los que el EI arremetió contra sus enemigos en la batalla de Mosul. Los drones realizaron labores de reconocimiento de objetivos y posterior guiado de los vehículos explosivos por las calles de la ciudad (Balkan, 2017).

La utilización de los drones como arma de guerra experimentó una evolución cuando se añadió cargas explosivas a los UAV, siendo estas liberadas sobre posiciones enemigas. Este modelo fue exportado a los combates del EIIL en Deir ez-Zor y a las ofensivas contra los kurdos en Siria.

Los incidentes de ataques con drones kamikazes con Visión en Primera Persona (FPV) fueron residuales al principio, aunque su frecuencia aumentaría con el tiempo (Lyle, 2019).

## 2.2. GUERRA DE UCRANIA

Otro escenario destacable fue el conflicto en el Donbás, iniciado en 2014. El papel inicial de los UAV fue reconocer objetivos que, posteriormente, la artillería hostigaría. Estos drones, equipados en ocasiones con medios de visión nocturna, comenzaron a ser conocidos por los militares de ambos bandos a causa de los zumbidos nocturnos, que solían venir inmediatamente acompañados de andanadas de las piezas enemigas.

Sin embargo, la evolución de los drones pequeños como armas de guerra entraría en una espiral de innovación después del inicio del frustrado ataque rusa contra Ucrania del 24 de febrero de 2022, y la subsiguiente guerra que, en noviembre de 2025, no parece tener un final próximo a la vista.

Al igual que se pudo ver en Siria, los drones fueron rápidamente modificados con remedios artesanales para cargar explosivos, como granadas o proyectiles de mortero, y arrojarlos sobre las posiciones defensivas enemigas. La primera diferencia que surgió en este teatro de operaciones fue el rápido surgimiento de ataques con drones con Visión en Primera Persona (FPV). Eran cuadricópteros con una carga explosiva con espoletas de impacto acopladas (Naber, 2025).

Este cambio de paradigma ofreció a ambos bandos la posibilidad de ejecutar acciones precisas contra objetivos concretos, facilitando el éxito de las operaciones, aunque conllevando la pérdida de al menos un aparato por acción.

El uso de drones aumentó de forma exponencial durante las primeras fases de la guerra, hasta alcanzar la situación actual, en la que ambos ejércitos cuentan con unidades especializadas en ataques con Sistemas Aéreos No Tripulados (UAS) integradas a muy bajo nivel. Por ejemplo, la 12ª Brigada de Fuerzas Especiales “Azov” del Ejército Ucraniano cuenta con una compañía de drones en cada batallón de combate, así como un batallón adicional de UAS para dar apoyo a la brigada. Algo similar se puede observar en otras unidades de ambos ejércitos (12ª Brigada de Fuerzas Especiales “Azov”, s.f.).

Tanto Ucrania como Rusia comenzaron en ese momento una pugna tecnológica, tratando de encontrar remedios contra los drones, a la vez que los mejoraban. Por ejemplo, se empezaron a desplegar redes antidrones en posiciones defensivas y vías logísticas principales, lo cual fue inmediatamente seguido por las tácticas tándem: un primer dron rompería la red, y el segundo entraría a por los objetivos (Méheut, 2025).

A fin de proteger los medios más importantes de cada bando, se extendió el uso de inhibidores para frustrar los intentos de destruirlos. Esto provocó un largo *impasse* en los frentes. Los equipos de drones comenzaron a tener cada vez menor tasa de efectividad,

a medida que los inhibidores se iban distribuyendo con mayor asiduidad. Ambas naciones trataron de encontrar soluciones a este sistema defensivo que, aunque no infalible, sí reducía en gran medida la capacidad operativa de los UAS (Loh, 2025).

Durante el verano de 2024, se comenzaron a registrar durante la invasión ucraniana del óblast de Kursk los primeros esfuerzos considerables con drones enlazados con el terminal que los controlaba mediante cables delgados de fibra óptica. La ventaja principal que tiene la conexión por cable es su inmunidad ante inhibidores. De igual modo se debe destacar que son indetectables por sistemas que se basen en la interceptación de ondas electromagnéticas, así como que aseguran una mejor conexión con el terminal de control, devolviendo imágenes de mayor calidad y facilitando su efectividad, pues mientras siga teniendo longitud de cable, no se perderá la conexión (Hambling, 2025).

En la actualidad, los avances tecnológicos parecen ir encaminados hacia el empleo, cada vez más común, de drones autónomos guiados por Inteligencia Artificial. La industria de defensa de Ucrania está trabajando en fabricar a gran escala modelos de drones que reconozcan las situaciones tácticas por sí mismos, las analicen adecuadamente, y tomen las decisiones óptimas para los intereses ucranianos. De idéntica manera está actuando el complejo militar industrial ruso. A finales de agosto de 2025, se produjeron al menos 100 incidentes de esta naturaleza (MacDonald, 2025; Boffey, 2025; Khomenko, 2024).

Al margen de las acciones en primera línea de combate, desde el inicio de la guerra de Ucrania se han sucedido las acciones a retaguardia enemiga, cada vez más complejas, y en las que los UAS de ambos actores juegan un papel crucial para la consecución de los objetivos.

Las lecciones aprendidas en Ucrania han inspirado las operaciones que se han sucedido en otros lugares del planeta. Por citar un ejemplo, durante la masacre del 7 de octubre de 2023 en el sur de Israel, el grupo Hamás atacó posiciones fronterizas de las Fuerzas de Defensa de Israel con UAV de pequeñas dimensiones (Page, 2025).

### **3. LA OPERACIÓN TELARAÑA**

#### **3.1. EL ATAQUE DEL 1 DE JUNIO DE 2025**

El 1 de junio de 2025, las bases aéreas rusas de Olenya, Ivanovo Severny, Dyagilevo, Ukrainka y Belaya amanecieron bajo un ataque por parte de fuerzas especiales ucranianas. No se trataba de misiles balísticos ni de drones de largo alcance, como los que Ucrania había utilizado frecuentemente hasta entonces. Enjambres de pequeños drones de Visión en Primera Persona (FPV) atacaron las posiciones de la Fuerza Aérea Rusa.

El objetivo del ataque era la flota de bombarderos estratégicos que Rusia había venido empleando de forma sistemática en su campaña de desgaste contra la infraestructura civil ucraniana. El saldo final fue la destrucción o incapacitación del 34% de la flota atacada. Además, estos modelos de aeronaves se encontraban fuera de producción desde 1993, dificultando la reconstrucción de la capacidad estratégica de largo alcance. En el plano económico, Ucrania asegura que el daño producido ascendería a alrededor de 7.000 millones de dólares (Gibson et al. 2025).



Debe ser destacado el hecho de que pequeños drones FPV hubieran atacado directamente bases aéreas enemigas extremadamente alejadas de la línea del frente, como la base de Ukrainka, que se encuentra a más de 5.800 km de la frontera internacionalmente reconocida de Ucrania, y a más de 6.000 km de la línea del frente. Para poner estas cifras en contexto, es una distancia superior a la que hay entre el centro de Madrid y Herat (Afganistán), y prácticamente la misma que hay entre Madrid y Baltimore, en Estados Unidos (EE. UU.).

El Servicio de Seguridad de Ucrania (SBU) logró atacar bases militares a más de 6.000 kilómetros empleando modelos de drones que suelen cumplir misiones tácticas muy próximas al frente, y cuya mayor debilidad es su dificultad para enlazar con el terminal de control. Fue posible porque los drones empleados en esta operación despegaron cerca de cada una de las bases aéreas. En el caso del ataque a la base aérea de Belaya (el mayor ataque de la operación, con 3 bombarderos Tu-95 y 4 bombarderos Tu-22M3 destruidos), los drones FPV despegaron desde una posición al sureste de la base a unos 8 kilómetros (Dempsey, 2025).

### 3.2. LA OPERACIÓN

La “Operación Telaraña” del Servicio de Seguridad de Ucrania (SBU) tuvo una fase de planificación y preparación de más de 18 meses, según el presidente ucraniano *Volodymyr Zelenskyy* (Zelenskyy, 2025). Se emplearon cuadricópteros con Visión en Primera Persona (FPV) “Osa”, de la empresa ucraniana *First Contact* (First Contact, 2025).

Los drones del modelo Osa se distinguen por la ubicación de sus componentes electrónicos bajo una cubierta exterior particularmente gruesa y por tener el puerto de alimentación en una posición fija, cuando la mayoría de los modelos de drones FPV empleados regularmente por las Fuerzas Armadas Ucranianas suelen tener un cuerpo “esquelético”, en el que los componentes electrónicos y el cableado suelen ir descubiertos. Después de considerar la complejidad de la misión, la distancia entre el lugar de preparación de la operación y los objetivos, y las condiciones climáticas diversas en las que se desarrollaría la infiltración, el SBU optó por el modelo más robusto.

Durante los 18 meses de preparación, el SBU consiguió introducir 117 drones Osa en la Federación Rusa. Una vez dentro del territorio enemigo, se creó una empresa pantalla de construcción dedicada a la edificación de viviendas modulares de madera para ocultar los movimientos. Estos módulos de vivienda contaban con un falso techo retráctil, en los que se ocultaron 9 filas de 4 drones cada una, para una capacidad total teórica de 36 drones por módulo. Paralelamente, también se ocultaron drones en contenedores de mercancías (Bondar, 2025).

En cada módulo también se instaló un sistema de control remoto, que actuaría de intermediario entre los 117 drones realizando el ataque y los 117 pilotos controlándolos desde Ucrania. El enlace entre los sistemas de control remoto y las posiciones de los operadores se pudo llevar a cabo a través de satélite.

Una vez ensamblados los “caballos de Troya”, el SBU contactó con empresas de transporte de mercancías rusas. Estas llevaron los drones Osa a los “puntos de entrega”

de los cargamentos, que finalmente fueron las ubicaciones dispuestas por el SBU para el despegue posterior de los drones.

A primera hora del 1 de junio de 2025, las cubiertas de los “caballos de Troya” ya infiltrados se levantaron, lo que permitió a los drones despegar y dirigirse a sus objetivos. Se difundieron numerosos vídeos de civiles rusos de estos módulos y contenedores con drones saliendo de ellos dirigidos hacia las nubes negras causadas por las explosiones de los que les precedieron.

Haciendo el balance global de la operación, unos 117 drones Osa, cuyo valor oscilaría entre 600 y 1.000 dólares por unidad, causaron unas pérdidas a la aviación rusa, y por tanto a todo el brazo armado del país, de 7.000 millones de dólares.

Este ataque supone una derrota sin paliativos para Rusia, que no solo sufrió estas pérdidas imposibles de reemplazar, sino que lo hizo de un modo que sacó a relucir las graves deficiencias tanto de la defensa aérea del país como de los esfuerzos de contrainteligencia. En términos de humillación, podría ser mayor que el ataque con dos drones al Kremlin del 3 de mayo de 2023 (Barnes et al., 2023).

Cabe señalar que todos los implicados ucranianos fueron exfiltrados del territorio ruso con anterioridad suficiente al ataque. De este modo, no solo se realizó la operación sin sufrir una sola baja propia, sino que Ucrania ahora cuenta con personal con la experiencia de ejecutar este tipo de acciones. Si esta operación tuvo una fase de planificación y preparación de 18 meses, no sería descabellado pensar que en estos precisos momentos se podría estar gestando el próximo ataque a gran escala contra la retaguardia rusa.

### 3.3. DIFERENCIAS CON OTRAS OPERACIONES SIMILARES

La Operación Telaraña no constituye en modo alguno el primer ataque con drones de pequeñas dimensiones contra infraestructuras críticas para la defensa nacional de un Estado. Los insurgentes en Irak han atacado durante años las posiciones del Ejército Iraquí y de los ejércitos de la coalición internacional contra el Estado Islámico con UAV. También los rebeldes sirios llevaron a cabo ataques con drones contra la base aérea rusa de Hmeimim, en la región leal al gobierno de Bashar Al-Asad de Latakia. No obstante, lo más destacable de esta acción es la profundidad del ataque dentro del territorio enemigo, la sofisticación técnica de su ejecución, y el hecho de que fuese contra bases con material crítico y escaso del segundo mayor ejército del planeta, en un contexto de conflicto bélico en el que los ataques a retaguardia constituían una dinámica constante del conflicto.

Ben Connable defiende que la operación ucraniana, aunque exitosa, debe interpretarse dentro de su contexto adecuado. Destaca que experiencias previas en Siria (Hmeimim), Irak, Yemen, y otros lugares revelan que los aeródromos pueden ser eficazmente protegidos contra estos ataques mediante una defensa aérea dispuesta por capas. Por tanto, no deberíamos caer en la tentación de calificar como revolución bélica lo que podría no ser más que un caso de fallo de seguridad aislado (Connable, 2025).

Es posible que se trate un fallo de planificación de la defensa aérea rusa como plantea Ben Connable. Sin embargo, hay que poner también en su contexto los ejemplos que el autor menciona.

Se analizará el caso con mayor disponibilidad de información: los múltiples ataques con drones contra la Base Aérea de Hmeimim, en Latakia (Siria). La instalación fue construida en 2015 para ser empleada como centro estratégico de la intervención rusa en Siria. Esta base ha sufrido una larga lista de ataques con medios UAV desde 2018 hasta el más reciente en enero de 2025.

El primero de estos ataques sucedió el 6 de enero de 2018, cuando 13 aeronaves no tripuladas de ala fija fueron interceptadas por los medios de guerra electrónica presentes en la base y posteriormente capturados, aunque algunos sí que tuvieron que ser derribados por medio de defensa antiaérea. Destacable es tanto la diferencia de números como de los medios empleados por los rebeldes con respecto a la Operación Telaraña (BBC, 2018).

A partir de ese momento, la base aérea comenzó a ser atacada de modo continuado hasta 2021, año en el que los ataques cesaron, salvo algún caso esporádico. Los medios oficiales rusos, posiblemente buscando el mayor rédito propagandístico, acostumbraron a dar datos de largos periodos de tiempo, y no tanto de ataques concretos. Durante agosto de 2018 la base fue atacada por 47 Vehículos Aéreos No Tripulados (UAV), y entre septiembre y octubre de 2018, el personal militar de la base derribó 50 UAV.

De este modo, los ataques de los grupos rebeldes sirios habrían sido de una escala que dista de ser superior a la capacidad de defensa rusa. Además, cabe entender que, en búsqueda de proteger el centro estratégico de su intervención militar en Siria, Rusia habría aumentado de modo muy significativo los medios de defensa aérea presentes en la base. Además, la Base de Hmeimim se encuentra a menos de 100 kilómetros de Idlib, la región siria con mayor presencia y control rebelde a lo largo de toda la guerra civil.

No serían, por tanto, comparables las experiencias de Hmeimim con lo sucedido en las bases atacadas por Ucrania el 1 de junio de 2025, dadas las diferencias en el contexto geográfico, nivel de alerta previo y complejidad de la acción.

El esfuerzo requerido por la Federación Rusa para haber protegido todas las bases aéreas, navales, y terrestres de su territorio adecuadamente, así como a cualquier infraestructura crítica susceptible de ser un objetivo militar sería inmenso. Esta dificultad se incrementa para un país en guerra contra su vecino al oeste, con las evidentes implicaciones que esto tiene a la hora de determinar el despliegue de las unidades con capacidades de defensa antiaérea.

### 3.4. CONSECUENCIAS

Al igual que ocurre teóricamente en la guerra naval, los ataques con drones están más centrados en tácticas de enjambre que en asegurar el impacto de cada dron individual. Esto resulta de lo ocurrido tanto en Ucrania, como en los ataques que ha realizado Irán contra Israel. Debemos por tanto concluir que los ataques con drones contra objetivos protegidos por medios antidrones basan su éxito en el enjambre (Price, 2025; Tangredi, 2023).

Es relevante considerar el papel determinante que tuvo la Inteligencia Artificial en la ejecución de la operación. A pesar de que oficialmente los drones fueron pilotados por operadores ucranianos, estos podrían haber empleado medios de navegación autónoma como previsión ante posibles pérdidas de enlace. De este modo, aunque los pilotos hubiesen perdido la conexión con los aparatos, estos habrían continuado su camino hacia las bases aéreas sin control humano ni señal de GPS. También habrían distinguido los objetivos desde la distancia (De Troullioud, 2025).

Durante la fase de preparación de la Operación Telaraña, a los drones se les programó para reconocer los medios aéreos que iban a atacar, y así resaltárselos al piloto para que colisionase el dron contra los lugares más sensibles para la integridad estructural de las aeronaves, por ejemplo, los depósitos de combustible. Estas capacidades habrían sido posteriormente puestas en práctica con aviones bombarderos fuera de servicio con los que Ucrania contaba en sus depósitos (Bondar, 2025).

De este modo, a pesar de que Ucrania hiciera uso de pilotos humanos para ejecutar esta operación, se evidencia que el nivel de implicación de la IA en el éxito de es innegable. También lleva a la pregunta de si la ejecución podría haberse llevado a cabo íntegramente por medios UAV autónomos. En esta ocasión no pudo emplearse, aunque atendiendo a los avances producidos, se puede concluir que en un futuro próximo se podrá emplear. Incluso cabría la posibilidad de que ya se está experimentando en este sentido. Los beneficios inmediatos serían determinantes para el éxito de futuras operaciones: posibilitar el empleo de enjambres gigantescos, varias veces mayores a los que se podrían ver en la actualidad, e incrementar enormemente la seguridad de la operación, evitando las señales enviadas desde el centro de control hasta los drones.

La Operación Telaraña podría considerarse una de las operaciones de infiltración más exitosas del siglo XXI. Es una acción que recibió reconocimiento por la comunidad occidental, aunque ahora no sea del todo consciente de las implicaciones a futuro de esta. El gobierno ruso salió rápidamente a condenar la acción como un atentado terrorista, pese a que se atacaron objetivos militares legítimos en un contexto de conflicto armado reconocido por ambos estados. No obstante, y con ocasión de las imágenes difundidas ese día, cabe reflexionar: ¿en qué se diferenciaría visualmente un ataque terrorista contra bases aéreas españolas de lo que sucedió en el interior del territorio de la Federación Rusa?

#### **4. LOS DRONES DE ATAQUE LLEGAN A SUDAMÉRICA**

Como dijo José Nemesio García Naranjo: “pobre México, tan lejos de Dios y tan cerca de Estados Unidos”. Esta afirmación bien podría extenderse a varias naciones americanas situadas al sur del río Grande, en particular aquellas donde hay una gran presencia de grupos de delincuencia organizada. Las malas condiciones económicas, unidas a la incesante demanda de sustancias ilícitas en mercados externos como EE. UU. o Europa, han conducido durante décadas al continente americano a enfrentamientos, guerras civiles e inestabilidad social. En ocasiones, se ha llegado a extremos como el de El Salvador, donde el 1,7% de la población total del país se encuentra encarcelada, en su mayoría por supuesta participación en el tráfico de sustancias y pertenencia a grupos de crimen organizado (Human Rights Watch, 2024).

El gobierno de los Estados Unidos denomina a algunos de estos grupos Organizaciones Criminales Transnacionales (OCT) por su poder e influencia. Unos cuentan con arsenal, personal y capacidades equiparables a algunos ejércitos nacionales, tales como el Cártel de Jalisco Nueva Generación (CJNG), liderado por Nemesio Oseguera Cervantes “el Mencho”. Otras organizaciones cuentan con una tasa de implantación operativa en los mercados criminales de más de 40 países, tales como el Cártel de Sinaloa (CDS) (Drug Enforcement Administration [DEA], 2025). El caso de este último grupo es paradigmático del control que ejercen sobre su territorio, pues un conflicto por el liderazgo del cártel iniciado en 2024 ha llevado a que el estado de Sinaloa se haya declarado en diversos momentos como zona de guerra por periodistas internacionales, causando al menos 1.900 muertes y 2.000 desapariciones en un año exclusivamente por este conflicto (Villegas, octubre 2025).

Estas organizaciones criminales han aprovechado los avances tecnológicos de las últimas décadas para sus operaciones. En concordancia con esto, se han sumado a la revolución de los drones, aplicándolos fundamentalmente para el desempeño de tres cometidos: vigilancia y seguridad, tráfico de mercancías y ataque directo.

Al igual que se ha podido vivir en Ucrania, Hispanoamérica ha experimentado un crecimiento exponencial en el uso de estos medios particularmente desde el año 2022. Los grupos de delincuencia organizada han analizado las experiencias en el este de Europa casi con tanto detenimiento como los ejércitos profesionales, sino incluso más. Los dos países sudamericanos con mayor presencia de drones en el contexto de la delincuencia organizada son México y Colombia.

#### 4.1. MÉXICO

Para analizar el empleo de los drones por parte de los grupos de crimen organizado en México, nos hemos de remontar a principios de la década de 2010. Fue en estos años cuando se empezaron a descubrir drones comerciales a los que se les daba el uso de vigilancia. A partir de ahí, se comenzó a explorar la posibilidad de transportar sustancias ilícitas cargadas en ellos.

En enero del año 2015, un dron cargado con 2 kilogramos y medio de metanfetamina se estrelló en la ciudad de Tijuana, México, cuando se disponía a cruzar la frontera con EE. UU. Hasta ese momento, las autoridades de control de fronteras de los EE. UU. no habían registrado ningún intento de contrabando empleando drones (Valencia, 2015).

Habría que esperar hasta 2017 para que aparecieran los primeros indicios de que las Organizaciones Criminales Transnacionales (OCT) podrían estar experimentando con el concepto de drones explosivos. Cuatro hombres que viajaban en un vehículo que había sido denunciado como robado fueron detenidos por la policía en el Estado de Guanajuato, en una zona que se encontraba “caliente” (disputada por más de un grupo de delincuencia organizada). Los cárteles de Sinaloa, Jalisco Nueva Generación y los Zetas tenían una importante presencia en Guanajuato, y se hallaban en conflicto por el control. Al inspeccionar el vehículo, hallaron un dron con “gran cantidad” (no describiendo con exactitud la cantidad) de explosivos adosados al cuerpo, y equipado con un iniciador que se activaba por radiofrecuencia (AFP, 2017).

La primera constancia de tentativas de ataques con drones se produjo el 9 de julio de 2018, cuando un Vehículos Aéreos No Tripulados (UAV) impactó contra la casa de Gerardo Manuel Sosa, secretario de Estado de Seguridad Pública de Baja California, en la localidad de Tecate. Este dron portaba dos granadas de fragmentación que finalmente no detonaron. Además, el secretario de estado no se hallaba en su domicilio en el momento del atentado (CNN Español, 2018).

La utilización de drones comenzó a aumentar gradualmente por todo el país, aunque sin ninguna organización concreta y mediante pequeñas acciones, a todas luces realizadas con materiales, equipos y procedimientos *ad hoc*.

Todo cambió en el año 2021, con el líder del grupo de 'los Deltas', Armando Gómez Núñez, alias 'Delta 1'. Los Deltas son un brazo armado del Cártel de Jalisco Nueva Generación que operó en la zona fronteriza entre los Estados de Jalisco y Michoacán. Armando Gómez creó la primera unidad de drones de ataque especializados, al mando de la cual estaría "el Flaco Drones", y una misteriosa integrante a la cual se apodó "Lady Drones", que fue detenida el 13 de agosto de 2025 (Secretaría de Defensa Nacional, 2024; Mendoza, 2025).

Esta nueva unidad de drones, junto a otras en diversos grupos criminales, comenzaron a operar de modo más técnico y sofisticado. Se empezó a llamar "droneros" a los operadores de medios Sistemas Aéreos No Tripulados (UAS), y se han requisado diversos parches de unidades "droneras" (Maza, 2025).

El esfuerzo en drones del Cártel de Jalisco Nueva Generación (CJNG) en la frontera entre Jalisco y Michoacán respondía a un conflicto contra la "Familia Michoacana", que no tardó en responder al grupo jalisciense estableciendo sus propias unidades de operadores de drones.

Actualmente, el uso de unidades de ataque con medios UAS se ha extendido a todo México, aunque los incidentes se concentran en los Estados de Michoacán y Guerrero. En lo que a los operadores respecta, el CJNG y la Familia Michoacana son las dos organizaciones más avanzadas en el empleo de drones. Detrás de estos dos vendría el Cártel de Sinaloa, y después el resto de los grupos criminales en diversas fases de evolución en este ámbito (Jaramillo, 2025).

El tipo de ataque con dron más común en los conflictos en México son los *droppers*, es decir, los que liberan cargas explosivas sobre un objetivo, siendo raro encontrar acciones realizadas con drones con Visión en Primera Persona (FPV), aunque cada vez son más comunes. Estos *droppers* son también empleados en labores de vigilancia, y hasta de contrabando o transporte de objetos de pequeñas dimensiones (Villegas, septiembre 2025).

En un principio, los ataques con drones eran generalmente dirigidos hacia otras organizaciones criminales, reportándose algún caso concreto de ataques contra personal de policía o de las Fuerzas Armadas Mexicanas. En 2021 se registraron 10 fallecidos, de los cuales 7 eran miembros de grupos criminales. Las víctimas disminuyeron en 2022 a 8 (Ziemer, 2025).



Los ataques con drones sufrieron un aumento considerable en 2023. Ese año, la cifra se elevó a 35, casi cinco veces más que el año anterior. Sin embargo, lo más aterrador no fue el aumento, sino la distribución de víctimas. De las 35, 27 eran civiles. Había comenzado una nueva era de los drones en México. Los grupos criminales estaban ahora usando los drones, ya no solo para atacar a enemigos directos, sino para sembrar el pánico en la población de los territorios “calientes”. En este periodo, hubo ataques directos contra pueblos en los Estados de Michoacán y Guerrero, en uno de los cuales aldeanos capturaron a un sicario de la Familia Michoacana (Grillo, 2024).

Este sicario, Fernando, realizó una declaración a periodistas en la que dio a entender que no solo es que los UAS hayan llegado a México para quedarse, sino que se va a aumentar su uso de aquí en adelante: “tienen *droneros*. Tienen gente especial para *dronear* (...). Tienen hartos (muchos) drones, así que, aunque una mula (persona dedicada al tráfico de objetos y mercancía oculta) pierda alguno no les importa (...). Como esto apenas va empezando” (Grillo, 2024).

Ha llegado a tal nivel la capacidad técnica de las OCT en el ámbito de los UAS, que ya se están empezando a ver los primeros indicios de un esfuerzo real por parte de las organizaciones criminales por invertir en medidas y unidades antidrones. Prueba de ello es que, en 2024 y en el contexto de la guerra civil sinaloense, un miembro de una de las facciones que se disputa el control del Cártel de Sinaloa, “los Mayitos” (la facción liderada por los hijos de Ismael “el Mayo” Zambada, detenido en 2024), fue fotografiado portando un sistema de inhibición anti UAS *Skyfend*, valorado en 100.000 dólares (Jiménez, 2025).

Aunque un único sistema de defensa antiaérea es insuficiente para contrarrestar el potencial destructivo de los drones de ataque, sí revela un esfuerzo por entrar en la carrera armamentística que tanto se puede ver en otros escenarios como el ucraniano.

En el plano de la lucha contra el empleo ilícito de los drones, el gobierno mexicano ha reaccionado dictando disposiciones para dificultar el acceso a los UAV. En 2019 se redactó la NOM-107-SCT3-2019, reguladora de los Sistemas de Aeronaves Pilotadas Remotamente (RPAS). En ella, todo aparato de más de 250 gramos debe estar registrado. Se prohíbe modificar los RPAS para posibilitar el transporte de mercancías peligrosas o para arrojar objetos. Esta medida, en un país donde hay regiones enteras donde el gobierno de facto está en manos de OCT, ha tenido escasa repercusión en la resolución del problema del uso de drones con fines criminales.

En el plano humanitario, las amenazas proferidas contra la población civil han llevado a varios desplazamientos de refugiados. En el año 2023, en torno a 600 residentes de Nuevo Caracol, Estado de Guerrero, tuvieron que abandonar sus domicilios por los continuos ataques con drones sobre la población (Ortiz, 2023).

## 4.2. COLOMBIA

Un escenario hispanoamericano en el que el empleo de drones por parte de organizaciones en enfrentamiento con el gobierno nacional está siendo cada vez más relevante es Colombia. Este país registró su primera muerte atribuible a drones de ataque en julio de 2024, en la que un niño de 10 años falleció y otras 12 personas fueron heridas cuando un

Vehículo Aéreo No Tripulado (UAV) atacó con una granada de fragmentación un campo de fútbol en El Platerado (Torres, 2024).

El principal responsable del empleo de drones en Colombia es el Ejército de Liberación Nacional, particularmente desde que lanzó su ofensiva sobre el Catatumbo a principios de 2025. Los ataques con drones son responsables en parte de la crisis de desplazados que se vivió en esta región, con más de 52.000 personas forzadas a abandonar sus hogares (ACNUR, 2025).

Una de las facciones disidentes de las Fuerzas Armadas Revolucionarias de Colombia Ejército del Pueblo (FARC-EP), las FARC-EP también han protagonizado atentados con drones, como los ataques en noviembre de 2024 y en julio y agosto de 2025 a tres Patrulleras de Apoyo Fluvial Pesado de la Armada Colombiana, en el río San Juan del Micay, Departamento del Cauca, o el derribo de un helicóptero antinarcóticos en Antioquia en agosto de 2025, con el fallecimiento de los 13 policías que iban en su interior (Saumeth, 2025; Torrado, 2025).

El 10 de junio de 2025, el autoproclamado Secretariado de Estado Mayor Central de las FARC-EP emitió un comunicado con 10 recomendaciones para la población civil, prensa y organismos humanitarios, con la finalidad de evitar incidentes de ataques a civiles. Entre estas se destacan mantener una distancia mínima de 500 metros con convoyes militares o de policía, y exigir a las Fuerzas Armadas que abandonen instalaciones colindantes con edificios de uso residencial (W Radio Colombia, 2025).

El número de víctimas por ataques de drones en Colombia continúa siendo menor que el de México, aunque en Colombia se están empezando a apreciar desde mediados de 2025 ataques de mucha mayor entidad, como los ya mencionados ataques a buques y helicópteros.

Los gobiernos enfrentados a enemigos con Sistemas Aéreos No Tripulados UAS en Sudamérica se han visto desbordados por el momento. Varios países, entre los que se encuentran Colombia, Perú y México, han comenzado a dotar a sus fuerzas armadas y de seguridad con sistemas de defensa antidrones, para poder al menos proteger sus bases e infraestructuras críticas.

Por su parte, hay gobiernos en el continente americano que están optando por combatir a los grupos de crimen organizado con drones. En Haití, una operación con drones del gobierno el 1 de marzo de 2025 se saldó con 80 bajas ese día, aunque no se ha podido confirmar que todos fueran miembros de organizaciones criminales. Uno de los líderes de las bandas de Puerto-Príncipe, Jimmy Cherizier, condenó el ataque, amenazando con responder con drones propios, pudiendo causar la muerte de “cualquier persona del país” (Vyas, 2025).

#### 4.3. SOLUCIONES PROPUESTAS

El problema al que se enfrentan los estados hispanoamericanos es de extrema gravedad, y desde diversas perspectivas se han recopilado tres recomendaciones que deberían constituir los principios rectores de la política anti UAS que desarrollen estas naciones: atacar las líneas de suministro, aprender de los expertos, e invertir en entrenamiento y tácticas (Ziemer, 2025).



Es necesario reconocer que la lucha contra las líneas de suministro de las organizaciones ilegales es inseparable e intrínseca a la lucha contra los propios grupos. Pese a ello, la victoria de los Estados, al menos en cuanto a los drones, habrá de venir necesariamente desde el enfoque del ataque a las líneas de suministro.

Se abre por tanto una oportunidad para, tal vez, tomar de inspiración la Operación *Grim Beeper*, llevada a cabo por los servicios de inteligencia de Israel mediante la cual se infiltraron en la cadena de suministro de “buscas” de Hezbolá con el resultado final que todos conocemos (Doran, 2024).

Por su parte, aprender de los expertos e invertir en investigación y tácticas supone extraer el máximo rendimiento posible de la información que pueden ofrecer los países que más estén inmiscuidos en este desarrollo: Ucrania, Rusia e Israel.

## 5. APLICACIÓN DE LAS LECCIONES

Se pueden extraer muchas lecciones de un análisis de las experiencias de Siria, Ucrania, Israel, México y Colombia. Las que consideramos que más se deben destacar son:

- A. Los UAS son especialmente efectivos si comparamos su precio y capacidad destructiva.
- B. El enlace por fibra óptica permite evitar la incapacitación de drones por dispositivos inhibidores de radiofrecuencias.
- C. La fuerza de una acción realizada por UAV generalmente fundamenta su éxito en la detección tardía y en la táctica de enjambre.
- D. El avance de la inteligencia artificial propicia la aparición de drones autónomos con capacidad de reconocer su entorno y designar sus objetivos.
- E. El empleo de drones permite retirar la máxima capacidad de integrantes de la operación antes de que se inicie, reduciendo las bajas propias a prácticamente nulas.

Estas lecciones tendrán que ser debidamente tenidas en cuenta a la hora de afrontar posibles empleos de los UAS como instrumentos terroristas.

Del mismo modo, se debe siempre tener en consideración que los grupos que tengan capacidad para emplear drones los van a utilizar. Esta tecnología y técnicas son fáciles de adaptar a diferentes modos de operación y entornos, como se ha demostrado con su reciente incorporación al escenario de la lucha contra el crimen organizado en Brasil. El 28 de octubre de 2025, en el marco de una operación contra la estructura del *Comando Vermelho* en Río de Janeiro, este utilizó drones de combate contra los agentes de las fuerzas de seguridad. El *Comando Vermelho* es la mayor organización de crimen organizado de Brasil, y ya ha incorporado a los Sistemas Aéreos No Tripulados (UAS) a sus operaciones (Braun, 2025).

## 5.1. LECCIONES APRENDIDAS EN ANTERIORES ATENTADOS

### 5.1.1. Atentados del 11 de septiembre

En el informe emitido por la Comisión de Investigación de los atentados del 11 de septiembre (11-S) del 22 de julio de 2004 (*National Commission on Terrorist Attacks*, 2004), el undécimo capítulo: “Previsión y Retrospección” realiza un juicio crítico detallando las principales 4 debilidades en el sistema de contrainteligencia y lucha antiterrorista de los EEUU que posibilitaron la comisión del mayor atentado por número de víctimas de la historia: falta de imaginación, política inadecuada frente a Al-Qaeda, mal uso de las capacidades del gobierno federal, y errores graves en la gestión operativa del ataque como tal. La política inadecuada y el mal uso de las capacidades responden más a cómo lidiar con un enemigo que surge, por lo que entendemos que se escapan del objetivo de este artículo.

De las dos que sí vamos a analizar, la más crítica es la falta de imaginación, pues la otra procede directa o indirectamente de esta. El primero de los errores fue la clasificación del riesgo que la comunidad de inteligencia de los EE. UU. hizo. El encargado de la oficina antiterrorista, Richard A. Clarke, argumentó en una nota del 4 de septiembre de 2001 que una parte de las agencias antiterroristas consideraban los atentados como “una molestia que mata a un número de estadounidenses cada 18-24 meses”. Aun los que sí consideraban el riesgo como real, como Clarke, redactaban supuestos hipotéticos en los que “cientos” de estadounidenses resultaban víctimas del terrorismo. Prácticamente nadie se imaginaba un posible escenario como el que finalmente ocurrió.

También se hace mención en el informe a que la comunidad de inteligencia ignoró casi completamente la posibilidad de que un avión fuese empleado como vehículo suicida, a pesar de que los ataques suicidas se habían estado convirtiendo en los más habituales en Medio Oriente. Si se hubiese realizado un ejercicio poniéndose en el lugar de un terrorista que quisiera hacer uso de un avión secuestrado, posiblemente se hubieran detectado los fallos de seguridad que se harían evidentes como consecuencia del 11-S. Es más, la cuestión se llegó a plantear en ocasiones por órganos ajenos a la comunidad de inteligencia, siendo en todos los casos desestimada por esta como extremadamente improbable. Esto se expuso en el informe de la Comisión de Investigación de los Atentados del 11 de septiembre, en las páginas 345 a 348 (*National Commission on Terrorist Attacks*, 2004).

No menos graves fueron los errores cometidos en el manejo operativo de las acciones que posibilitaron la comisión del atentado. Se destaca la falta de coordinación entre agencias federales, principalmente la Agencia Central de Inteligencia (CIA) y el Buró Federal de Investigaciones (FBI). Todas las acciones preparatorias fueron detectadas por alguna institución estadounidense (la reunión previa en Kuala Lumpur, las entradas de los sospechosos al territorio americano, la formación como pilotos de los sospechosos, y un largo etcétera), mas no hubo una buena comunicación de estas informaciones, lo que facilitó que el FBI no considerase incluir la presencia de los sospechosos que tenían localizados al informe de riesgo de ataques inminentes.

### **5.1.2. Atentados de Barcelona y Cambrils**

Algo parecido pudo suceder en los atentados que lamentablemente sacudieron España en 2017 en Barcelona y Cambrils. Las autoridades competentes habrían decidido no actuar sobre el oficio del entonces Comisario General de Seguridad Ciudadana de la Policía Nacional, Florentino Villabona Madera, en la que se instaba a instalar “grandes maceteros o bolardos en los accesos (a lugares con alta concurrencia de personas)” (Redacción Barcelona La Vanguardia, 2017). En este caso, la imaginación de las Fuerzas y Cuerpos de Seguridad no falló, aunque sí la de los encargados de poner en práctica sus recomendaciones. Las mismas carencias se vieron en lo relativo a la coordinación policial, pudiendo haber sido obviado un supuesto aviso enviado por la CIA el 25 de mayo de 2017 en la que alertaba de la voluntad del EIIL de atacar contra La Rambla de Barcelona (El Periódico Barcelona, 2017).

### **5.1.3. Resumen de las lecciones aprendidas**

La falta de imaginación y coordinación de las instituciones son dos de los pecados capitales en la lucha antiterrorista. La nueva era de la tecnología nos obliga a replantearnos el modo de actuar de potenciales terroristas de aquí en adelante, con el probable empleo de drones, inteligencia artificial, o la letal combinación de ambos en las próximas tentativas de ataques terroristas, además de otras herramientas aún en desarrollo.

## **5.2. POSIBILIDADES DE ATENTADOS TERRORISTAS CON DRONES**

### **5.2.1. Ataques contra aglomeraciones de personas**

En cuanto a los atentados contra grandes aglomeraciones de personas, consideramos reseñable el tiroteo masivo de Las Vegas del 1 de octubre de 2017, en la que un sujeto se hizo con un arsenal valorado en 95.000 dólares y abrió fuego desde una suite del hotel Mandalay Bay hacia un festival al aire libre aledaño al hotel, con el resultado de 60 víctimas mortales y 867 heridos. Este incidente demostró lo ineficientes que pueden ser las medidas de control de acceso a una instalación, si el riesgo viene desde arriba (Las Vegas Metropolitan Police Department, 2018).

No es necesario realizar un enorme esfuerzo de imaginación para pensar cómo de destructivo hubiera podido llegar a ser este mismo ataque, pero empleando Vehículos Aéreos No Tripulados (UAV) que arrojaran cargas explosivas de varios kilos sobre la multitud, más aun teniendo en cuenta que el atentado sucedió de noche, lo que en la realidad ya tuvo consecuencias trágicas, pues sobre los presentes se impuso un clima de caos total.

### **5.2.2. Ataques contra individuos**

La posibilidad de atentados contra altas autoridades del Estado tampoco debe ser descartada. El presidente de Venezuela, Nicolás Maduro, sufrió un atentado con drones explosivos durante un desfile militar el 4 de agosto de 2018 (El Mundo, 2018). De este modo, no solo es que estos ataques sean posibles, sino que ya se han intentado.

Sabemos que, aunque difícil, no es imposible aproximarse peligrosamente a altas autoridades, como demostró el intento de asesinato al entonces candidato a la presidencia de los EE. UU., Donald Trump, el 13 de julio de 2024. Thomas Crooks logró acercarse armado con un fusil AR-15 a menos de 150 metros de Trump, y alcanzó incluso disparar ocho cartuchos antes de ser abatido por agentes del Servicio Secreto (*Task Force on the Attempted Assassination of Donald J. Trump*, 2024).

Un hipotético ataque con dron no hubiese tenido que acercarse tanto como un tirador, pudiendo camuflarse más fácilmente en los alrededores antes de lanzar un dron guiado por fibra óptica o un enjambre de drones equipados de software de guiado por Inteligencia Artificial con objetivo Donald Trump.

### 5.2.3. Ataques contra la aviación y otros sectores

El sector aéreo también puede ser objeto de esta tipología de atentado. De un modo similar a la Operación Telaraña, en un futuro los drones podrían reconocer los motores, depósitos de combustible o la ventana de la cabina de un aparato y colisionar contra ellos en el momento del despegue o aterrizaje. Considerando que un Boeing 737-800 o un Airbus A320 (los dos modelos más comunes de aviación comercial) pueden transportar más de 180 pasajeros, un impacto efectivo contra un solo avión se convertiría inmediatamente en el segundo mayor atentado de la historia de España.

Las opciones son incontables: trenes detenidos por un primer dron y que posteriormente empiezan a ser atacados con secundarios, ataques combinando métodos ya conocidos de terrorismo y empleando los drones para atacar a las personas que huyen por cuellos de botella, por citar algunos ejemplos.

### 5.3. ATACAR LA LÍNEA DE SUMINISTRO

Las ventajas para los terroristas también son innumerables: no tienen como *conditio sine qua non* la muerte del ejecutor, las acciones preparatorias no se realizan en el mismo lugar del ataque, dificultando su detección temprana (nadie puede encontrar una mochila bomba que no está ahí) y son objetos ampliamente vendidos en los mercados civiles, por lo que no levantan tantas sospechas como otros métodos.

Quizás parte de una correcta perspectiva a la hora de luchar contra los atentados con drones es reconocer que detenerlos una vez iniciada la ejecución va a ser una tarea cada vez más compleja, si no directamente imposible en ocasiones; al igual que Rusia no puede tener grandes unidades de defensa antiaérea en cada metro cuadrado de su territorio, nosotros tampoco. No habría que enfrentarse a los drones cuando ya están volando hacia su objetivo, sino cuando están dentro de una caja siendo transportados de un lugar a otro.

### 5.4. FASES DELICADAS DEL PROCESO DE PREPARACIÓN DE UN ATENTADO CON UAS

Hemos podido detectar al menos 4 procesos delicados en la preparación de una acción terrorista con drones: la obtención de los drones, el entrenamiento de los pilotos, la programación de los drones y la obtención de los explosivos.

La obtención de grandes cantidades de Sistemas Aéreos No Tripulados (UAS) en la Unión Europea, y más concretamente en España, no sería la parte más delicada de la operación. A pesar de que es obligatorio estar registrado y tener licencia para pilotar drones de un peso superior a 250 g, estas restricciones no aplican para el simple acto de comprarlo. Esto saca a relucir una deficiencia. El acopio excesivo y fuera de lo lógico de estos productos debería siempre estar vigilado, lo cual se ve profundamente perjudicado por esta libertad para su compra. Más aún cuando se pueden realizar en cualquier establecimiento de la Unión Europea, o incluso en otras naciones, en tanto que no se exige permiso de aduanas para la importación de UAS para uso personal. También se debe considerar los drones resultantes del trabajo de impresoras 3D.

El entrenamiento de los pilotos podría suponer una buena oportunidad para interrumpir la comisión del atentado, particularmente si tratan de obtenerlo por cauces legales. Ya los servicios de inteligencia americanos pudieron haber estado cerca de frustrar el 11-S, al menos del modo en el que los terroristas lo habían organizado, cuando el FBI emitió un informe en julio de 2001 sobre el interés que estaban adquiriendo sospechosos de ser yihadistas por formación de vuelo al que titularon: “Extremista Islámico Aprende a Volar” (National Commission on Terrorist Attacks, 2004).

Habría que estar especialmente atentos a lo que suceda cuando finalicen las hostilidades en Ucrania, y los pilotos de drones de ataque ucranianos y rusos traten de reinsertarse en la sociedad. Hasta ahora, los estudios realizados sobre los efectos psicológicos de operar drones de ataque se han centrado casi en exclusiva en los pilotos de bombarderos no tripulados estadounidenses, que por la naturaleza de sus acciones están sometidos a un nivel de estrés considerablemente inferior a los operadores ucranianos y rusos.

La programación de los aparatos para que sigan unas instrucciones concretas, mediante el empleo de Inteligencia Artificial (IA) requiere unos conocimientos avanzados en varias áreas técnicas, como programación en Python y C++, formación de IA, robótica y electrónica. No es un conocimiento particularmente costoso en el plano temporal, pero un interés repentino de un sujeto sospechoso en estas áreas del conocimiento debe ser una señal de alerta inmediata.

Al igual que en el punto anterior, habrá que plantear la posibilidad de que en la preparación de estas operaciones colaboren, o incluso participen activamente, veteranos de la guerra de Ucrania, u otras similares en cuanto al uso masivo de drones. Los equipos de drones de estos conflictos bélicos tienen un conocimiento técnico sobre la adaptación de drones de paquete al cumplimiento de misiones específicas que exceden por una amplia diferencia aquellos con los que puede contar prácticamente cualquier otro individuo.

Por último, la adquisición de explosivos constituiría, como es lógico, el proceso más frágil de todo el *iter criminis*. Esto se acentúa cuando se toma en consideración que los Sistemas Aéreos No Tripulados (UAS), por sus características técnicas, no pueden portar cargas excesivamente pesadas, forzando a los posibles terroristas a recurrir a sustancias explosivas con mayor potencial de detonación, pudiendo reducirse en cierto modo la búsqueda de estas tentativas.

## 6. CONCLUSIONES

A. Los drones han llegado para quedarse. No hay duda de que su uso se incrementará enormemente. Las experiencias de los países que se han visto inmersos en conflictos con drones deberán ser añadidas a los procedimientos propios.

B. La Operación Telaraña llevada a cabo por el Servicio de Seguridad de Ucrania (SBU) contra la flota estratégica de largo alcance rusa demostró la versatilidad de las acciones con drones contra objetivos situados miles de kilómetros detrás de la línea de frente. Estos medios han demostrado su capacidad para ser infiltrados, distribuidos y operados a gran distancia. Extrapolando esta experiencia, se deduce la capacidad destructiva de un grupo decidido a eliminar una infraestructura en una zona civil, dados los recursos necesarios.

C. El empleo de Inteligencia Artificial (IA) en esta operación, acompañada de las instancias ya documentadas del empleo de estas herramientas, modifican drásticamente el escenario de las amenazas futuras. Los drones de ataque acabarán siendo dispositivos explosivos guiados con IA con las herramientas requeridas para diferenciar aliados de enemigos, y eliminar a estos.

D. Las Organizaciones Criminales Transnacionales de Hispanoamérica se han adentrado con paso decidido a la batalla tecnológica por el dominio de los cielos. Sus asentadas redes de tráfico de toda clase de materiales y sustancias les han permitido acumular grandes cantidades de Sistemas Aéreos No Tripulados (UAS), que están desempeñando labores de vigilancia, transporte y ataque. Desde el año 2021 cuentan con unidades propias especializadas y actualmente están empezando a invertir en material antidrones.

Los ataques, aunque tímidos y reducidos en un principio, están adquiriendo una dimensión cada vez más ambiciosa, atacando incluso convoyes enemigos en movimiento. También la población civil ha sufrido el resultado de la introducción de estas tecnologías en los conflictos entre grupos criminales, con ataques directos e indiscriminados contra poblaciones cada vez más frecuentes en México y Colombia.

En este último país, las fuerzas armadas y las fuerzas y cuerpos de seguridad están siendo objetos de ataques considerables, y que podrían ser los tanteos previos a otras acciones de una envergadura aún no vista en este continente.

E. La experiencia en todos los teatros ha demostrado que el éxito de una acción con drones contra un objetivo defendido radica en el enjambre.

F. En Ucrania se ha demostrado que los drones de ataque son recursos extremadamente útiles en el contexto de una guerra, y en Sudamérica que pueden servir para sembrar el terror en poblaciones y unidades de seguridad de los Estados, más es así si sus operaciones responden a los intereses de grandes organizaciones con una capacidad logística y militar superior a algunos Estados soberanos.

Parece una realidad que tarde o temprano estas formas de cometer acciones violentas llegará a Occidente, así como a España. Debemos estar preparados, y hacer memoria de los errores cometidos anteriormente para no repetirlos en el futuro.

G. La imaginación y la capacidad de gestionar estos escenarios son dos requisitos fundamentales para afrontar las nuevas amenazas. Varios atentados terroristas pasados se han podido consumir por análisis de riesgo incorrectos. La aparición de drones con IA abre la puerta a que los terroristas puedan encontrar oportunidades donde anteriormente les hubiera resultado impensable, tanto a ellos como a las fuerzas de seguridad.

Quizás la manera más efectiva de enfrentarles podría ser interceptando las tentativas durante su fase de preparación. Tanto el acopio de drones, como la formación de los pilotos, la programación de los UAS y la obtención de explosivos parecerían ser momentos idóneos para frustrar los intentos de ataques contra población civil.

La seguridad no debe ser tampoco despreciada. Ataques de pequeña entidad serían más difíciles de detectar, aunque al contrario que los complejos sí podrían ser detenidos durante su ejecución.

Por último, debemos recalcar la urgente necesidad de aprovechar la experiencia que están adquiriendo en este sector los países que actualmente se encuentran en conflictos donde la presencia y uso de drones son habituales. Esa información podría ser decisiva en las futuras investigaciones contra células terroristas decididas a perpetrar un ataque contra nuestro territorio.



## 7. REFERENCIAS BIBLIOGRÁFICAS

- 12ª Brigada de Fuerzas Especiales “Azov” (s.f.). *About Azov*. Recuperado el 3 de septiembre de 2025 de <https://azov.org.ua/en/about-azov/>
- ACNUR (2025). *Urge fortalecer la respuesta frente al desplazamiento masivo sin precedentes en el Catatumbo, Colombia*. <https://www.acnur.org/noticias/comunicados-de-prensa/acnur-urge-fortalecer-la-respuesta-frente-al-desplazamiento-masivo-sin-precedentes-en-el-catatumbo-colombia>
- AFP (2017). Un dron explosivo, el último artefacto del crimen organizado en México. *El País*. [https://elpais.com/internacional/2017/10/24/mexico/1508802891\\_139491.html](https://elpais.com/internacional/2017/10/24/mexico/1508802891_139491.html)
- BBC (2018). Syria war: Russia thwarts drone attack on Hmeimim airbase. *BBC*. <https://www.bbc.com/news/world-europe-42595184>
- Barnes, J. E., Entous, A., Schmitt, E., Troianovski, A. (2023). Ukrainians Were Likely Behind Kremlin Drone Attack, U.S. Officials Say. *The New York Times*. <https://www.nytimes.com/2023/05/24/us/politics/ukraine-kremlin-drone-attack.html>
- Balkan, S. (2017). DAESH’s Drone Strategy. Technology and the Rise of Innovative Terrorism. *Foundation for Political, Economic and Social Research (SETA)*. <https://media.setav.org/en/file/2017/08/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism.pdf>
- Boffey, D. (2025). Killing Machines: how Russia and Ukraine’s race to perfect deadly pilotless drones could harm us all. *The Guardian*. <https://www.theguardian.com/world/2025/jun/25/ukraine-russia-autonomous-drones-ai>
- Bondar, K. (2025). How Ukraine’s Operation Spider’s Web” Redefines Asymmetric Warfare. *Center for Strategic & International Studies*. <https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare>
- Braun, J. y Toledo, L. F. (2025). Comando Vermelho: cómo drones y fusiles importados acaban en manos del crimen organizado en Brasil y están transformando el conflicto urbano. *BBC*. <https://www.bbc.com/mundo/articles/c4g32d0r5o>
- Connable, B. (2025). Putting Operation Spider’s Web in Context. *Irregular Warfare*. <http://irregularwarfare.org/articles/putting-operation-spiders-web-in-context/>



- De Troullioud de Lanversin, J. (2025). Ukrainian attack on Russian bombers show how cheap drones could upset global security. *Bulletin of the Atomic Scientists*. <https://thebulletin.org/2025/06/ukrainian-attack-on-russian-bombers-shows-how-cheap-drones-could-upset-global-security/#:~:text=The%20drones%20were%20likely%20%E2%80%9COsa,for%20Strategic%20and%20International%20Studies>
- Dempsey, J. (2025). Operation Spiderweb: an assessment on Russian Aerospace Force losses. *International Institute for Strategic Studies*. <https://www.iiss.org/online-analysis/military-balance/2025/062/operation-spiderweb-an-assessment-of-russian-aerospace-forces-losses/>
- Department of Defense (2000). DOD Directive 12/2000.
- Doran, M. (2024). The Brilliance of “Operation Grim Beeper”. *Hudson Institute*. <https://www.hudson.org/technology/brilliance-operation-grim-beeper-lebanon-pager-explosion-israel-iran-michael-doran>
- Drug Enforcement Administration (2025). *2025 National Drug Threat Assessment*. <https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf>
- El Mundo (2018). Maduro denuncia "un intento de asesinato" con drones explosivos y culpa al presidente Santos. *El Mundo*. <https://www.elmundo.es/internacional/2018/08/05/5b662beeca4741d0498b4648.html>
- El Periódico Barcelona (2017). Texto íntegro de la alerta de atentado en Barcelona de la CIA a los Mossos. *El Periódico*. <https://www.elperiodico.com/es/politica/20170831/texto-integro-alerta-cia-mossos-atentado-barcelona-rambla-6255316>
- First Contact (2025). *High-Acrobatic UAV Osa*. Recuperado el 4 de septiembre de 2025 de <https://firstcontact.biz/en/projects/high-acrobatic-uav-osa/>
- Gibson, O., Harvey, A., Novikov, D., Harvard, C. y Stepanenko, K. (2025). Russian Offensive Campaign Assessment, June 1, 2025. *Institute for the Study of War*. <https://understandingwar.org/research/russia/russian-offensive-campaign-assessment-june-1-2025/>
- Grillo, I. (2024). La Guerra de Drones en Guerrero. *CrashOut by Ioan Grillo*. <https://www.crashoutmedia.com/p/la-guerra-de-drones-entre-carteles>
- Hambling, D. (2025). New Drone Tactics Sealed Russian Victory in Kursk. *Forbes*. <https://www.forbes.com/sites/davidhambling/2025/03/17/new-drone-tactics-sealed-russian-victory-in-kursk/>
- Hambling, D. (2016). How Islamic State is using consumer drones. *BBC*. <https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones>

- Human Rights Watch (2024). *Informe para el Examen Periódico Universal de El Salvador (48° período de sesiones de las Naciones Unidas; 4° ciclo)*. <https://www.hrw.org/es/news/2024/07/30/informe-para-el-examen-periodico-universal-de-el-salvador>
- Jaramillo, J. C. (2025). Drones Fuel Criminal Arms Race in Latin America. *Insight Crime*. <https://insightcrime.org/news/drones-fuel-criminal-arms-race-latin-america/>
- Jiménez, X. (2025). ‘La Mayiza’ pone en jaque a fuerzas armadas en Sinaloa con equipo anti dron de élite. *Milenio*. <https://www.milenio.com/policia/mayiza-combate-fuerzas-armadas-equipo-anti-dron-elite>
- Khomenko, I. (2024). How Ukraine is Using AI Drones to Outsmart Russia on the Battlefield. *United24 Media*. <https://united24media.com/latest-news/how-ukraine-is-using-ai-drones-to-outsmart-russia-on-the-battlefield-3833>
- Las Vegas Metropolitan Police Department (2018). *LVMPD Criminal Investigative Report of the 1 October Mass Casualty Shooting*. <https://www.lvmpd.com/home/showpublisheddocument/134/638298568313170000>
- Loh, M. (2025). Ukraine’s drone jammers are proving decisive amid a new push on Russian soil, pro-Kremlin milbloggers say. *Business Insider*. <https://www.businessinsider.com/ukraine-drone-jammers-killing-it-new-kursk-push-russian-bloggers-2025-1>
- Lyle, P. (2019). Air Power Proliferation: How Commercial-off-the-Shelf Drones are Being Used by Violent Extremist Organizations to Influence the Future of Warfare in the Air. *Air and Space Power Review*, 22(3). <https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/aspr-vol22-iss3-6-pdf/>
- MacDonald, A. (2025). AI-Powered Drone Swarms Have Now Entered the Battlefield. *The Wall Street Journal*. <https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05>
- Maza, J. (2025). Drones y letalidad tecnológica de los cárteles mexicanos. *Consejo Mexicano de Asuntos Internacionales*. <https://www.consejomexicano.org/mediateca/articulo/7275>
- Méheut, C. (2025). Ukraine Turns to Fishing Nets to Catch Russian Drones. *The New York Times*. <https://www.nytimes.com/2025/07/07/world/europe/ukraine-russia-drones-nets.html>
- Mendoza López, D. (2025). Golpean al CJNG en Campeche: caen “El 80”, “Lady Drones” y tres sicarios tras operativo en Champotón. *Infobae*. <https://www.infobae.com/mexico/2025/08/14/golpean-al-cjng-en-campeche-caen-el-80lady-drones-y-tres-sicarios-tras-operativo-en-champoton/>

- National Commission on Terrorist Attacks (2004). *The 9/11 Commission Report*. <https://www.9-11commission.gov/report/911Report.pdf>
- Naber, I. (2025). Why Ukraine Remains the World's Most Innovative War Machine. *Politico*. <https://www.politico.com/news/magazine/2025/08/27/ukraine-drones-war-russia-00514712>
- Ortiz, J. (2023). El Caracol: el pueblo guerrerense asediado por narcodrones. *La Silla Rota*. <https://lasillarota.com/estados/2023/9/4/el-caracol-el-pueblo-guerrerense-asediado-por-narcodrones-445996.html>
- Page, J. M. (2025). Drones and the Hamas-led Attack of 7 October 2023: Innovation and Implications. *Perspectives on Terrorism*. <https://www.jstor.org/stable/27372135>
- Price, R. E. (2025). Defining Swarm: A Critical Step Toward Harnessing the Power of Autonomous Systems. *Military Review Online Exclusive*. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2025/Defining-Swarm/Defining-Swarms-UA.pdf>
- Redacción Barcelona La Vanguardia (2017). El documento con el que la Policía recomendó colocar bolardos en accesos a lugares concurridos. *La Vanguardia*. <https://www.lavanguardia.com/politica/20170819/43665066008/documento-policia-recomendo-instalar-bolardos-accesos-lugares-concurridos.html>
- Reuter, C. (2000). *The V2, and the Russian and American Rocket Program*. S.R. Research & Publishing.
- Salinas, A. (2018). Dron con granadas cae en casa del secretario de Seguridad Pública de Baja California. *Excelsior*. <https://www.excelsior.com.mx/nacional/dron-con-granadas-cae-en-casa-del-secretario-de-seguridad-publica-de-baja-california>
- Saumeth, E. (2025). Las FARC atacan con drones una tercera patrullera fluvial de la Armada de Colombia. *Infodefensa*. <https://www.infodefensa.com/texto-diario/mostrar/5404281/125-colombia>
- Secretaría de Defensa Nacional (SEDENA) (2024). *Ejército Mexicano y Guardia Nacional detuvieron a Armando "N" alias "Delta 1", presunto líder del Cártel Jalisco Nueva Generación en Michoacán y Jalisco*. <https://www.gob.mx/defensa/prensa/ejercito-mexicano-y-guardia-nacional-detuvieron-a-armando-n-alias-delta-1-presunto-lider-del?tab=>
- Skinner, B. F. (1960). Pigeons in a pelican. *American Psychologist*. American Psychological Association. <https://www.appstate.edu/~steelekm/classes/psy3214/Documents/Skinner1960.pdf>
- Tangredi, S. J. (enero 2023). Bigger Fleets Win. *Proceedings*. <https://www.usni.org/magazines/proceedings/2023/january/bigger-fleets-win>

- Task Force on the Attempted Assassination of Donald J. Trump (2025). *Final Report Findings and Recommendations*. <https://taskforce.house.gov/sites/evo-subsites/july13taskforce.house.gov/files/evo-media-document/12-5-2024-Final-Report-Redacted.pdf>
- Torrado, S. (2025). Las disidencias multiplican los ataques con drones y encienden las alarmas en Colombia. *El País*. <https://elpais.com/america-colombia/2025-08-30/las-disidencias-multiplican-los-ataques-con-drones-y-encienden-las-alarmas-en-colombia.html>
- Torres, M. (2024). Un niño muere tras un ataque con drones de las disidencias de las FARC en el Cauca. *CNN Español*. <https://cnnespanol.cnn.com/2024/07/24/nino-muere-ataque-drones-disidencias-farc-cauca-colombia-orix>
- Valencia, N. (2015). Drone carrying drugs crashes south of U.S. border. *CNN*. <https://edition.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border>
- Villegas, P. (octubre 2025). En medio de la guerra del cártel, los trabajadores funerarios cargan con el dolor de Sinaloa. *The New York Times*. <https://www.nytimes.com/es/2025/10/24/espanol/america-latina/sinaloa-muertes-trabajadores-funerarios.html>
- Villegas, P. (septiembre 2025). Drones y explosivos improvisados: los cárteles de México adoptan armas de guerra moderna. *The New York Times*. <https://www.nytimes.com/es/2025/09/01/espanol/america-latina/mexico-carteles-armas.html>
- Vyas, K. (2025). Haiti's Beleaguered Government Launches Drones Against Gangs. *The Wall Street Journal*. [https://www.wsj.com/world/americas/haiti-drones-gangs-fight-27e8341f?gaa\\_at=eafs&gaa\\_n=ASWzDAh20VgfmnFWwEE7OjowH1KxYc34z1aFI1uRw1vF-bKPi6aj4r7cWJlndm9cN1U%3D&gaa\\_ts=6841c7eb&gaa\\_sig=rJSPFiTqfMVMvHpXOVI9jsTqFd52rHCtmsgOdyDTpuRUVJ13ks5cvK5\\_LMvUMG6mn7gI\\_qSmKfkG5KLkeR4UAg%3D%3D](https://www.wsj.com/world/americas/haiti-drones-gangs-fight-27e8341f?gaa_at=eafs&gaa_n=ASWzDAh20VgfmnFWwEE7OjowH1KxYc34z1aFI1uRw1vF-bKPi6aj4r7cWJlndm9cN1U%3D&gaa_ts=6841c7eb&gaa_sig=rJSPFiTqfMVMvHpXOVI9jsTqFd52rHCtmsgOdyDTpuRUVJ13ks5cvK5_LMvUMG6mn7gI_qSmKfkG5KLkeR4UAg%3D%3D)
- W Radio Colombia [@WRadioColombia]. (10 de junio de 2025). #NoticiaW | Tras la cadena de atentados en Cauca y Valle del Cauca, el Estado Mayor Central de las FARC emitió [Recomendaciones a la población civil]. X. <https://x.com/WRadioColombia/status/1932474602267021560>
- Zelenskyy, V (1 de junio de 2025). Discurso a la Nación sobre el Ataque con Drones de la Operación Telaraña [Transcripción]. American Rhetoric. <https://www.americanrhetoric.com/speeches/volodymyrzelenskyoperationspiderweb.htm>
- Ziemer, H. (2025). Illicit Innovation: Latin America Is Not Prepared to Fight Criminal Drones. *Center for Strategic & International Studies*. <https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones>

## **8. NORMATIVA**

Reglamento Delegado (UE) 2019/945 de la Comisión, de 12 de marzo de 2019, sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas. 11 de junio de 2019. DOUE núm. 152.

Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS), y se modifican diversas normas reglamentarias en materia de control a la importación de determinados productos respecto a las normas aplicables en materia de seguridad de los productos; demostraciones aéreas civiles; lucha contra incendios y búsqueda y salvamento y requisitos en materia de aeronavegabilidad y licencias para otras actividades aeronáuticas; matriculación de aeronaves civiles; compatibilidad electromagnética de los equipos eléctricos y electrónicos; Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea; y notificación de sucesos de la aviación civil. 5 de junio de 2024. BOE núm. 136.

NORMA Oficial Mexicana NOM-107-SCT3-2019, Que establece los requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el espacio aéreo mexicano. 14 de noviembre de 2019.

