Sistema global contra drones.

Autor: Cebrián de Barrio, José Antonio.

Directora: Fernández Gavilanes, Milagros.

Contacto: jac@interior.es

Resumen:

El crecimiento exponencial en las tecnologías 'drone', la gran cantidad de modelos de ámbito comercial, diferentes usos para los que son útiles, unido a la reducción de costes de compra y mantenimiento, facilidad de pilotaje y programación, incluyendo el desarrollo legislativo, hace que cada vez más empresas, organismos públicos, particulares, etc, se planteen la utilización de este tipo de aeronaves. Por este motivo, las Fuerzas y Cuerpos de Seguridad han de estar preparadas para hacer frente al uso malintencionado de este tipo de aeronaves.

Inicialmente se han definido las siguientes fases para hacer frente a la posible amenaza:

1. Detección: se detecta algo extraño, inicialmente no se puede saber si se trata de un dron, a dónde se dirige, las intenciones que tiene, etc.
2. Identificación: discernir si realmente se trata de un dron y tratar de obtener el mayor número de datos posibles del mismo. Incluyendo la posición del piloto.
3. Seguimiento: dará indicios de a dónde se dirige y posibles intenciones.
4. Neutralización: en caso necesario.
5. Inteligencia: todas estas fases han de disponer de una cierta inteligencia que ayuden al operador a tomar decisiones en tiempo real.

El 11 de Julio de 2019, en España se produjo un punto de inflexión, la Secretaría de Estado de Seguridad firmó una resolución por la que se declaraba de emergencia la contratación de un servicio, llamado Sistema Global Contra Drones (SIGLO-CD), con el objetivo de detectar, identificar y seguir drones comerciales en el área Metropolitana de Madrid, y en su caso neutralizar si se considera que amenaza a algunas de las mayores instituciones del Estado.

Palabras clave: Drone, Contradrones, CUAs, Seguridad Ciudadana, Siglo-CD.

---

1. Introducción

«*Lo consiguieron porque no sabían que era imposible*» Jean Cocteau.

Gracias a la velocidad a la que se están produciendo los avances tecnológicos, nos encontramos que, en el mercado de los drones, hay una gran variedad de marcas y modelos **'comerciales'** de coste reducido, facilidad de mantenimiento y pilotaje, posibilidad de programar diferentes funciones, entre ellas, las rutas mediante *waypoints*, añadiendo los diferentes usos para los que son útiles, incluyendo una legislación que permite que cada vez más empresas, organismos públicos, particulares, etc., se planteen la utilización de este tipo de aeronaves para diversos objetivos.

El problema es que la delincuencia organizada también trata de aprovechar los avances tecnológicos y este tipo de aeronaves son cada vez más utilizadas con fines ilegales. Desde el punto de vista estadístico, el uso 'no legal', 'alegal', 'ilegal', en la mayoría de los casos es por desconocimiento de la ley, por 'imprudencia'. Existen otros casos en los que conscientes de la ilegalidad del vuelo, estos no son conscientes de las posibles consecuencias, para ellos (sanciones), ni para terceros (daños colaterales en caso de accidente). El siguiente escalón es el uso de este tipo de tecnología para favorecer actividades ilegales, como, introducir droga en un centro penitenciario, invadir la intimidad de las personas y una gran variedad de comportamientos. Finalmente, en los casos más graves, el uso de estas aeronaves se hace para producir atentados. Por todos estos motivos las Fuerzas y Cuerpos de Seguridad, tienen que estar preparados tecnológicamente para proteger la Seguridad Ciudadana y las Libertades Públicas.

El objetivo del presente trabajo es doble.

1. Hacer una comparación de los diferentes sistemas que existen para neutralizar el uso malintencionado de los 'drones comerciales'.
2. En segundo lugar, se plantea como habría que desplegar una solución contradrones 'C-UAVs'.

Al ser una tecnología reciente, existe relativamente muy poca documentación al respecto, por lo que todo lo expuesto se basa en la experiencia personal.

2. Drones

Dron es la adaptación al español del inglés *drone* (abeja macho o zángano), para referirse a los vehículos aéreos no tripulado. Ha sido este año cuando ha empezado a figurar la palabra en el diccionario de la Real Academia de la Lengua. Los drones tienen diferentes denominaciones: UAV, UAS, RPA, RPAS…

Igualmente, hay diversas clasificaciones, las más conocidas son las basadas en el peso (clasificación OTAN) y por forma (ala fija, multirrotores, globos y dirigible). En la Figura 1, vemos la clasificación OTAN.

Class I w < 150	Small w > 20 kg	Tactical Unit (employs launch system)	h ≤ 5000 AGL	50 (LOS)	Luna, Hermes 90
	Mini 2 ≤ w ≤ 20 kg	Tactical Unit (manual launch)	h ≤ 3000 AGL	25 (LOS)	ScanEagle, Skylark, Raven, DH3, Aladin, Strix
	Micro w < 2	Tactical Patrol/section, Individual (single operator)	h ≤ 200 AGL	5 (LOS)	Black Widow

Figura 1. Clasificación OTAN. Fuente: Plan Director de RPAS de 2015 (DGAM)

El interés de las FFCCS para proteger la Seguridad Ciudadana se centra en los de clase 1, y dentro de ellos, los 'micro' y 'mini', ya que este tipo de drones son utilizados por delincuentes, bandas organizadas y organizaciones terroristas. DAESH e ISIS, han empleado drones comerciales con pequeñas modificaciones, para cometer atentados. En España hasta el momento, 'solo' se ha detectado un intento de atentado terrorista utilizando este tipo de tecnologías.

Por lo expuesto, cuando se detecta un vuelo no autorizado, inicialmente se desconoce la intención del piloto, por lo que debe ser tratada como una posible 'amenaza' hasta descartar que se trate de un peligro real. Téngase en cuenta, igualmente, que un vuelo lúdico cerca de un aeropuerto, se convierte en un 'peligro' grave, aunque no hay ninguna intención de causar daño.

En definitiva, las FFCCS han de estar preparados para prevenir, detectar, identificar y, en su caso, neutralizar este tipo de amenazas; diferenciando entre *security* y *safety*.

a) *Security*: evitar el uso de estas aeronaves en vuelos no autorizados, o para cometer acciones ilegales.
b) *Safety*: evitando los daños que estás aeronaves puedan producir a terceros por su uso inadecuado. Pero también a la hora de neutralizar, daños producidos nunca deben ser iguales o mayores de los que se quieren evitar.

Partimos de la premisa de que 'la seguridad 100% no existe', por lo que el punto de partida, será analizar cuáles son los drones comerciales más vendidos y centrarnos inicialmente en estos. Al respecto, tres marcas de drones comerciales ocupan más del 90% de las ventas y en el caso de España, podemos decir que más del 95% se concentra en DJI (90%), Parrot y Yuneec. El motivo es sencillo: precio bajo, facilidad de pilotaje y mantenimiento, aumento de las prestaciones, cargas de pago de mayor calidad.

3. Fases para hacer frente a la posible amenaza

Para conseguir neutralizar la posible amenaza, se han definido las siguientes fases, tal y como recoge la Figura 2:

- Detección: se detecta algo extraño, inicialmente no se puede saber si se trata de un dron, a dónde se dirige, las intenciones que tiene, etc. Tendremos que diferenciar entre 'falso positivo', detección no real o equivocada que hace saltar la alarma, y falso negativo, dron real no detectado, hay que reducir a cero este tipo de falsas alarmas, desde el punto de vista de la seguridad una amenaza real no detectada, es inasumible; ambos tipos de falsas alarmas son

inversamente proporcionales, por lo que para reducir a cero los falsos negativos, debemos aumentar la sensibilidad del detector, con lo que aumentarán los falsos positivos.

- Identificación: discernir si realmente se trata de un dron y tratar de obtener el mayor número de datos posibles del mismo. Incluyendo la posición del piloto.
- Seguimiento: dará indicios de a dónde se dirige y posibles intenciones.
- Neutralización: en caso necesario.
- Inteligencia: todas estas fases han de disponer de una cierta inteligencia que ayuden al operador a tomar decisiones en tiempo real.

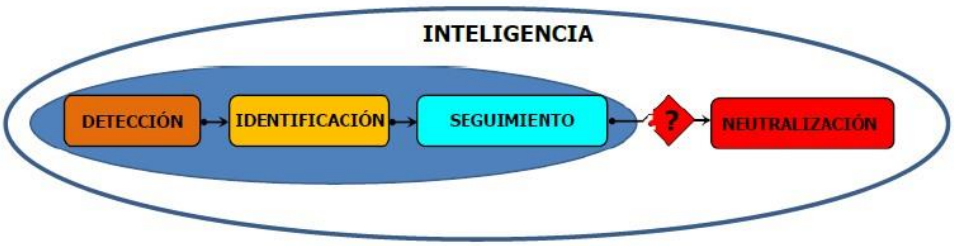

Figura 1. Fases para para neutralizar un dron.

4. Clasificación de las tecnologías de detección e identificación.

Podemos distinguir diferentes clasificaciones atendiendo a:

Sonido o ultrasonido.

Mediante la marca acústica característica que dejan este tipo de aeronaves, el problema es la distancia de detección que se vuelve crítica en entornos urbanos. No son soluciones muy populares debido a la escasa distancia de detección.

Sistemas ópticos.

Solución bastante extendida, sobre todo en la fase de identificación. Como sistema único de detección ha sido descartado, ya que para detectar a larga distancia se necesita que la distancia focal de los objetivos sea alta, reduciendo el ángulo de captación.

Radar activo.

Basados en el efecto *Doppler*, esto es, detectan el cambio de frecuencia de onda aparente de un objeto con movimiento con respecto un observador. Teóricamente funcionan bastante bien en entornos no urbanos, las distancias de detección son altas, necesitan un *software* de apoyo para clasificar las alarmas y hay que ajustar la sensibilidad para detectar los actuales drones de tamaño pequeño.

Radar pasivo.

Utilizan las señales emitidas por otros sistemas radio como ‘iluminadores de oportunidad’ en lugar de un transmisor propio. Se aprovechan infraestructuras ya desplegadas como ‘iluminadores’, siendo las más comunes la DVB (T y S), LTE, GSM, radio FM, GPS.

Sistemas de radiofrecuencias.

Escuchan las señales de radio en determinadas frecuencias, al tener clasificadas las tramas que se envían entre el *handcontrol* (piloto) y el dron, permite una detección bastante precisa. Constan de una

o varias antenas para recibir ondas de radio, para intentar detectar la comunicación entre un dron y su controlador. En 2017 DJI empieza a comercializar el sistema de detección Aeroscope, el cual detecta en un radio de 5Km con las antenas básicas (carezco de datos de dB), todos los drones de DJI y al descifrar la trama se obtienen datos precisos del modelo, número de serie, altura de vuelo, velocidad, etc.

Inteligencia.

Es importante que los futuros desarrollos incluyan inteligencia que ayuden al operador a clasificar las alarmas, esto es algoritmos de *machine-learning*, *deep-learning*, aprendizaje neuronal, que estudien patrones y en base a ellos mostrar probabilidades de intenciones.

5. Clasificación de las tecnologías de neutralización

Los sistemas de neutralización los podemos dividir en dos grandes bloques: cinéticos y no cinéticos.

Sistemas cinéticos.

Mayoritariamente dispositivos balísticos y similares.

- Utilización de munición no letal.
- Sistemas bloqueadores del vuelo basado en redes.
- Sistemas dron contra dron y sus variantes.
- Hard killing, balística convencional.

El problema fundamental de estos sistemas es que hay que estar cerca de la amenaza y la distancia de efectividad es muy escasa, dependen fundamentalmente de la pericia y reacción del operador.

Sistemas no cinéticos.

Dentro de este bloque podemos encontrarnos con:

- Bombardeo electromagnético de alta potencia. Basado en la utilización de microondas de alta potencia (HPM) que generan un pulso electromagnético (EMP) de frecuencias comprendidas entre 1 y 10GHz, enviadas directivamente. Son efectivos a distancias cortas, pudiendo generar graves daños colaterales en los dispositivos electrónicos y en las personas.
- Hack. Tomar el control del dron remotamente mediante técnicas de hacking; hay que estudiar el enlace entre el *handcontrol* y el dron. Son soluciones ideales, pero presentan diversos problemas, suelen ser caras y tardías.
- Spoofing GPS. Suplantar la señal GPS del dron, permitiendo llevarlo a zona segura, medida muy eficaz si el dron está programado para volar mediante waypoints. No está permitido en ningún caso este tipo de medida por legislación.
- Láser. Dispositivo óptico de alta potencia que produce un haz de luz coherente (muy focalizado). Destruye la estructura y la electrónica.
- Inhibidores de frecuencia. Es uno de los métodos más utilizados en estos momentos por su eficacia, fácil manejo, despliegue y precio. Son dispositivos que transmiten una gran cantidad de energía de radiofrecuencia hacia el dron o handcontrol, anulando la señal por lo que el drone deja de recibir instrucciones.

6. Pruebas reales de sistemas

Una vez analizadas las tecnologías existentes, se realizaron pruebas reales en diferentes entornos, destacando:

- Pruebas de evaluación de sistemas contra-drones - Aeropuerto de Asturias celebradas entre los días 14 al 18, del mes de septiembre de 2020.
- Participación en la prueba de campo de la licitación de la Liga Nacional de Fútbol Profesional (LaLiga) en agosto de 2021.

Pruebas en el Aeropuerto de Asturias.

Detección:

1. apantallada por un camión de bomberos.
2. apantallada por un edificio.
3. drones volando a baja cota.
4. drones volando a alta cota.
5. drones volando a distancia.
6. drones volando en modo autónomo.
7. detección de enjambres formados por drones autorizados y no autorizados.

En el siguiente gráfico se ven los resultados globales obtenidos por las diferentes empresas sobre un total de 100. El color amarillo indica detección mediante radiofrecuencia, el naranja detección radar y el verde ambas.

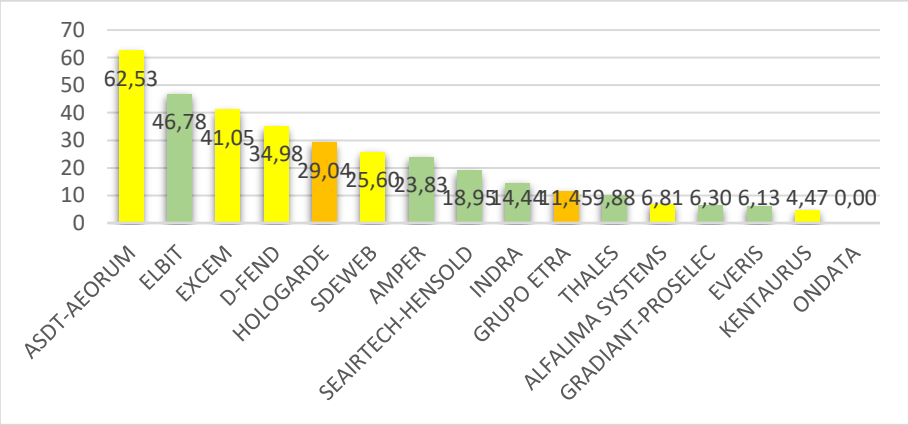

Figura 2. Resultados Asturias Global

Globalmente se puede observar que solo una empresa (el 5,5%) supera el 50% y solo seis empresas (el 33%) de dieciocho superan el 25%, resultados realmente malos desde el punto de vista de la seguridad, esto significa que de cada cuatro drones ‘comerciales’ que vuelan solo detectamos uno.

7. Siglo-CD

La Secretaría de Estado de Seguridad (SES) dispuso el año 2019 el diseño y la implementación de una plataforma tecnológica que pudiera llevar al desarrollo de un sistema integral contra drones, como protección ante hechos presuntamente ilícitos (vuelos imprudentes o con intención ilegal), así como

intrusiones en la privacidad personal, uso por crimen organizado y en los casos más graves, posibles acciones terroristas. La Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), fue la encargada de poner en marcha el Sistema Global Contra Drones (en adelante, SiGlo-CD). A continuación, vamos a desglosar las fases llevadas a cabo:

Fase 0, inicial.

El 11 de Julio de 2019 se firmó, por parte de la Secretaría de Estado de Seguridad, la resolución por la que se declaraba de emergencia la contratación del servicio de un sistema global.

La premisa inicial fue huir de sistemas stand-alone, por lo que se decidió basarse en la arquitectura cliente-servidor, donde los detectores y neutralizadores serían periféricos del sistema y se podrían instalar en el lugar más adecuado; todas las soluciones tenían que ser interoperables, independientemente del fabricante. La segunda premisa fue, hay que proteger el mayor número de ciudades e infraestructuras, con la mayor eficacia posible, por lo que la balanza calidad-precio es fundamental. Esta arquitectura cliente-servidor, se articula en torno a servidores dedicados pertenecientes a un CPD Principal (Sede Central), sobre el que transmiten y reciben información a través de una VPN mallada (no todos los sistemas, los más críticos se conectan mediante APN) los diferentes detectores, neutralizadores y usuarios de la red.

Los sistemas de detección seleccionados inicialmente, son pasivos y están basados en detección de radiofrecuencias (RF), ya que el entorno en que se desplegaron es urbano, también permiten obtener datos de marca, modelo, número de serie, *tracking*…, de los drones comerciales más extendidos, siendo una solución bastante eficaz. Su radio de cobertura es superior a 10Km. La Figura 3 muestra la detección de un drone en el barrio de Hortaleza de Madrid. …

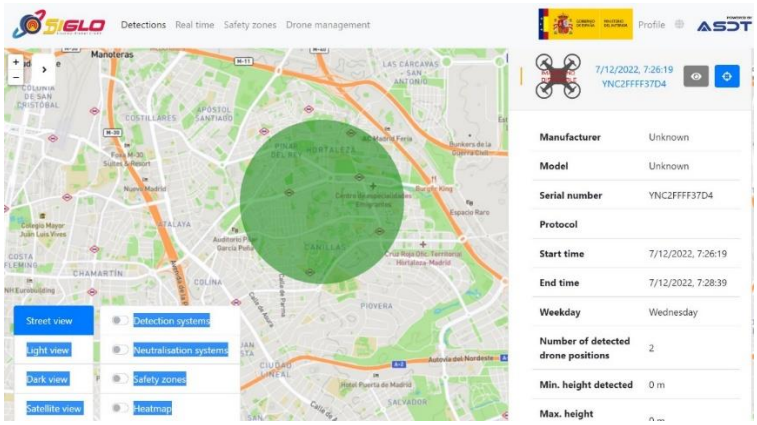

Figura 2. Captura real de pantalla, detectores en Madrid.

Respecto a los sistemas de neutralización, se seleccionaron los basados en *Jamming*, por las mismas razones que se han descrito. Salvo excepciones, se han seleccionado antenas directivas, para evitar al máximo los daños colaterales que este tipo de soluciones pueden causar.

El Centro de mando y control, permite la gestión de usuarios. Tiene dos vistas principales sobre un mapa GIS, tipo GoogleMaps: detecciones en tiempo real, historial de detecciones.

Fase 1

El contrato fue adjudicado en el mes de julio de 2022 y hay de plazo hasta el 31 de diciembre de 2023 suministrar y realizar el siguiente despliegue: 13 puestos de mando y control, 3 sistemas

estacionarios de detección, 10 sistemas portátiles de detección con módulo DJI, 9 sistemas estacionarios de neutralización direccional, 12 sistemas de neutralización de mano, 4 sistemas portátiles de neutralización omnidireccional.

Fase 2

Actualmente en Intervención, plazo de ejecución de 2023 a 2025. En la Fase dos se pretende poder desplegar el sistema en 32 ciudades españolas con antenas fijas, incluyendo 86 maletas de detección portátiles.

8. Estadísticas.

Durante el pasado 2021, se han detectado un total de 14.266 vuelos de drones en el casco urbano de Madrid.

9. Conclusiones.

Tras analizar más de cien soluciones existentes en el mercado se llegó a la conclusión de que, no existen soluciones globales para dar respuesta a todas las situaciones; la gran mayoría son soluciones *stand-alone*, pero hay muchos escenarios diferentes, con características muy diferentes. Por lo que el sistema debe ser escalable, modular, integrable, adaptable al lugar y a la situación.

- Integral. Todos los elementos del Sistema, independientemente del fabricante, formarán parte de un todo.
- Modular. El Sistema estará formado por diferentes subsistemas de detección, identificación, seguimiento y mitigación de drones. Formado por diferentes piezas, como un puzle, se irán seleccionando las piezas adecuadas dependiendo de la situación y la zona a proteger.
- Escalable. La infraestructura debe ser escalable con el fin de extender y optimizar la plataforma TIC con el tiempo y garantizar su disponibilidad y sostenibilidad en futuras ampliaciones.
- Adaptable: los sistemas se van a desplegar en diferentes lugares y situaciones, por lo que los mismos han de adaptarse a circunstancias cambiantes (como trabajar en zona urbana o no urbana, o ser fijo o móvil, entre otros.

En base a los resultados obtenidos en las pruebas y teniendo en cuenta la balanza calidad-precio, para soluciones globales, a día de hoy, los mejores sistemas de detección son los basados en radiofrecuencias y los de neutralización lo basados en inhibición.

Futuro

El software de mando y control deberá incorporar ayudas y capacidades de procesamiento basadas en técnicas de Inteligencia Artificial.

- Algoritmos de inteligencia artificial, que permitan la toma de decisiones, de modo rápido e intuitiva.
- “Previsión de zonas de intercepciones de drones”, en función de los datos proporcionados, basado en patrones del histórico de vuelos con características similares.
- Funcionalidad ‘predicción de la acción del piloto’ y predicción de trayectoria de vuelo, basada en la velocidad del dron, ubicación, franja horario y expediente del dron, entre otros.

Figura 3. Logo de Siglo-CD

Referencias.

Para la realización de este resumen, no se ha consultado ninguna referencia, salvo la Figura 1 obtenida del Plan Director de RPAS de 2015 (DGAM).