Universidad Zaragoza
1542

Trabajo Fin de Grado

Estudio de Sistemas Anti-Drones: Detección y Neutralización de drones

Autor

Juan Carlos Vereda Ruiz

Directores

Dra. Dña. Mónica Delgado Gracia
Tte. D. Federico Santana Vázquez

Centro Universitario de la Defensa-Academia General Militar

2022

REVERSO PORTADA

Agradecimientos

Quiero agradecer a todos aquellos, que de una u otra forma, han posibilitado la elaboración del presente trabajo, especialmente a mi tutora académica la Dra. Dña. Mónica Delgado Gracia y tutor militar Tte. D. Federico Santana Vázquez, a la Compañía de Transmisiones nº 18 y a todos los profesores del Centro Universitario de la Defensa como responsables de mi formación para la obtención del título del grado de Ingeniería de Organización Industrial

No quiero olvidarme en este agradecimiento de mi familia, por lo que quiero dedicar este trabajo a ellos, que siempre han estado cerca de mí y me han apoyado en todo momento, durante el tiempo de estancia en la Academia, para conseguir mi sueño de ser Teniente del Ejército de Tierra.

PÁGINA INTENCIONADAMENTE EN BLANCO

Resumen

Los Sistemas de Aeronaves no Tripuladas (*Unmanned Aircraft Systems*, *UAS*) han experimentado, en los últimos años, una proliferación exponencial y no siempre la finalidad de uso de éstos ha supuesto una actividad lícita. Dada la gran variedad de cualidades de que disponen este tipo de dispositivos, se convierten en una amenaza significativa cuando son utilizados con intenciones maliciosas. Contrabando, tráfico de drogas, tareas de espionaje, ataques terroristas, portadores de armas incluso de destrucción masiva, son algunos de los fines delictivos en los que se pueden utilizar los drones.

La forma impersonal y remota en la que estos dispositivos son operados, les confiere una ejecución de las acciones sin apenas riesgos. Si a esto le unimos la facilidad de manejo y lo económico y fácil que resulta su adquisición, constituyen un arma extremadamente peligrosa en manos terroristas. Esta amenaza no resulta ajena a las Fuerzas Armadas, que ha adquirido algunos sistemas anti-dron para protección de instalaciones fijas, además de otros portátiles, para protección temporal de objetivos.

En el análisis de la amenaza realizado, se han considerado aspectos tales como el tamaño del dron , el propósito de actuación maliciosa, las formas de guiado y el entorno de actuación. Estos aspectos condicionarán la configuración del sistema anti-dron necesario para una adecuada protección.

Respecto del concepto operativo del sistema C-UAS (*Counter Unmanned Aircraft Systems*), se han descrito las acciones que se realizan con la finalidad de protección frente a la amenaza. Se incluyen en este concepto la vigilancia, el mando y control y la reacción. En la operación de vigilancia, se incluye la situación global del dron y su seguimiento. En la operación de mando y control se realiza principalmente la identificación de la amenaza como requisito previo al apoyo a la decisión. Finalmente se procede a la reacción, donde se desarrollan medidas de neutralización *Softkill* (electrónicas) y/o *Hardkill* (cinéticas).

Tras la revisión de diferentes sistemas C-UAS, se ha realizado, en primer lugar, un análisis DAFO para valorar si resulta adecuado la adquisición de estos sistemas, para la protección de instalaciones militares fijas, en zonas urbanas y aisladas. En segundo lugar, se ha determinado el sistema más adecuado para la protección de estas instalaciones, mediante análisis multicriterio de los sistemas analizados.

PÁGINA INTENCIONADAMENTE EN BLANCO

Abstract

Unmanned Aircraft Systems (UAS) have experienced, in recent years, an exponential proliferation and the purpose of their use has not always been a legal activity. Given the abilities these aircraft have, they have become a significant threat when they are used with malicious intentions. Smuggling drugs, human trafficking, espionage, terrorist attacks, and carrying weapons of mass destruction are some of the criminal purposes for which drones can be used.

The impersonal and remote way these devices operated gives them the ability to execute actions with little risk. In addition to their ease of handling, the cheap cost to produce, and loosely regulated acquisition process, they constitute an extremely dangerous weapon in terrorist hands. This threat is not unknown to the Armed Forces, which is why they have acquired some anti-drone systems to protect fixed installations, as well as other portable ones, for temporary protection of objectives.

In the analysis of the threat carried out, aspects such as the drone's size, the purpose of malicious action, the forms of guidance, and the environment of action have been considered. These aspects will determine the configuration of the anti-drone system necessary for adequate protection.

Regarding the operational concept of the C-UAS system (*Counter Unmanned Aircraft Systems*), the actions that are carried out with the purpose of protection against the threat have been described. Included in this concept are surveillance, command and control, and reaction. In the surveillance operation, the global situation of the drone and its tracking is included. In the command-and-control operation, the identification of the threat is mainly carried out as a prerequisite for decision support. Finally, the reaction proceeds, where *Softkill* (electronic) and/or *Hardkill* (kinetic) neutralization measures are developed.

After reviewing different C-UAS systems, a SWOT analysis has been carried out first to assess whether the acquisition of these systems is appropriate for the protection of fixed military installations in urban and isolated areas. Secondly, the most suitable system for the protection of these installations has been determined through a multi-criteria analysis of the analyzed systems.

.

PÁGINA INTENCIONADAMENTE EN BLANCO

Palabras clave

Sistema Anti-dron: Los sistemas anti-dron, son un conjunto de equipos y software que permiten bloquear o eliminar del espacio aéreo a un dron no autorizado.

Dron: Vehículo aéreo no tripulado, más apropiadamente RPAS (*Remotely Piloted Aircraft System*)

PÁGINA INTENCIONADAMENTE EN BLANCO

Índice

Agradecimientos I
Resumen III
Abstract V
Palabras clave VII
Índice de figuras XI
Índice de tablas XIII
Abreviaturas, siglas y acrónimos XV
1. Introducción 1
1.1. Antecedentes 1
1.2. Objetivos y alcance 2
1.3. Ámbito de aplicación 2
2. Metodología 3
2.1. Revisión bibliográfica 3
2.2. Entrevista a expertos 3
2.3. Investigación comparativa de las soluciones tecnológicas anti-dron del mercado 4
3. Revisión bibliográfica 5
3.1. Análisis del dron 5
3.1.1. Tamaño del dron 5
3.1.2. Propósito del dron 7
3.1.3. Entorno y localización del dron 7
3.1.4. Guiado del dron 8
3.2. Concepto operativo de las soluciones de los sistemas anti-dron 9
3.2.1. Operación de vigilancia 9
3.2.2. Mando y control y ayuda a la decisión 14
3.2.3. Reacción 14
3.3. Soluciones de diferentes tipos de sistemas anti-dron 16
3.3.1. Sistema AUDS de Blighter 16
3.3.2. Anti-dron portátil Dronedefender de Battelle 17
3.3.3. Sistema ARMS de Indra 17
3.3.4. Sistema CERVUS de Gradiant 19
3.3.5. Sistema Aeroscope de DJI 20
3.3.6. Sistema Horus Captor de Thales 21
3.3.7. Sistema ADRIAN de electrónica Roma 22

3.3.8. Sistema Drone Guard de Elta Systems 22
3.3.9. Sistema Leonidas de Epirus 24
4. Análisis DAFO 27
5. Análisis multicriterio 29
5.1. Identificación y selección de los criterios 29
5.2. Selección del método de análisis multicriterio 30
5.3. Determinación del peso relativo de cada criterio 30
5.4. Realización de la ponderación de criterios 31
5.5. Identificación e implementación de la solución seleccionada 32
6. Conclusión 33
Bibliografía 35
Anexos 37
Anexo 1: Entrevista a experto de Indra D. Francisco Vázquez Vázquez (Director de Desarrollo de Productos de Defensa y Vigilancia Electrónica de Indra) 37
Anexo 2: Entrevista a experto en UAS del Regimiento de Artillería Antiaérea 71 40
Anexo 3: Entrevista a experto en UAS del Regimiento de Guerra Electrónica 31 42
Anexo 4: Entrevista a experto en UAS del BCG de COMGEMEL 45
Anexo 5: Entrevista a experto en UAS del BCG de COMGEMEL 48

Índice de figuras

Figura 1. Clasificación de drones según su tamaño. Fuente OTAN 5
Figura 2. Automn drone. Fuente: Indra 6
Figura 3. Dron Skywalker X8. Fuente: Indra 6
Figura 4. Dron DJI Phanton 3 Fuente: Indra 6
Figura 5. Dron multicóptero Hydra-12. Fuente: Directindustry 6
Figura 6. Clasificación según firma Doppler. Fuente: Indra 10
Figura 7. Campos de trabajo de cámara infrarroja y visible. Fuente: Indra 10
Figura 8. Modo vigilancia del sistema anti-dron. Fuente: Indra 11
Figura 9. Sistema anti-dron. Fuente: Indra 12
Figura 10. Sistema anti-dron. Fuente: Indra 12
Figura 11. Imagen IR de ejemplo para tracking (seguimiento). Fuente: Indra 13
Figura 12. Imagen IR de ejemplo para clasificación. Fuente: Indra 13
Figura 13. Hardkill. Fuente: Indra 15
Figura 14. Radar, cámara de video EO e inhibidor direccional RF. Fuente: Bligter 16
Figura 15. Fusil Dronedefender. Fuente: Battelle 17
Figura 16. Conjunto optrónico sistema ARMS. Fuente: Indra 18
Figura 17. Captura mediante malla de dron hostil. Fuente Indra 19
Figura 18. Configuración en modo portátil. Fuente: Revista Ejército de Tierra nº 962 20
Figura 19. Equipo anti-dron portátil. Fuente: Thales 21
Figura 20. ELM-2026BF. Fuente: Elta Systems 23
Figura 21. Detector RF. Fuente: Elta Systems 23
Figura 22. POPStar. Fuente: Elta Systems 23
Figura 23. ELK-7009. Fuente Elta Systems 24
Figura 24. ELK-7009A. Fuente: Elta Systems 24
Figura 25. Smartsight. Fuente: Elta Systems 24
Figura 26. Drone Kill Drone. Fuente: Elta Systems 24
Figura 27. Rocknet. Fuente: Elta Systems 24
Figura 28. Simulación de funcionamiento Sistema Leonidas. Fuente: Epirus 24
Figura 29. Sitema Leonidas montado sobre remolque. Fuente: Epirus 25
Figura 30. Matriz DAFO. Fuente: elaboración propia 27

PÁGINA INTENCIONADAMENTE EN BLANCO

Índice de tablas

Tabla 1. Resumen de características de los sistemas analizados 26
Tabla 2. Criterios sensores 29
Tabla 3. Criterios mando y control 29
Tabla 4. Criterios Medidas SoftKill 29
Tabla 5. Criterios HardKill 29
Tabla 6. Pesos relativos de cada criterio 30
Tabla 7. Ponderación de criterios de los sistemas 31

PÁGINA INTENCIONADAMENTE EN BLANCO

Abreviaturas, siglas y acrónimos

2D	2 dimensiones
3D	3 dimensiones
ADRIAN	Anti-Drone Interception Acquisition Neutralization
AESA	Agencia Estatal de Seguridad Aérea
AMO	Análisis multicriterio
ATZ	Zona de tránsito de aeródromo
BCG	Batallón del Cuartel General
BOE	Boletín Oficial de Estado
C-UAS	Counter Unmanned Aerial Systems
CCAL	Centro de Coordinación del Apoyo Logístico
CCD	Charge Coupled Device (Dispositivo de carga acoplada)
COMGEMEL	Comandancia General de Melilla
DAFO	Debilidades, Fortalezas, Oportunidades y Amenazas
DEA	Administración de Control de Drogas
EO	Electróptico
EO/IR	Electro Óptica/Infrarrojo
EW	Guerra Electrónica
FIZ	Zonas de información de vuelo
FMCW	Frequency Modulated Continuous Wave (Onda continua modulada en frecuencia)
FOV	Field of view (Campo de vision)
FPV	Visión en primera persona
GIS	Sistema de Información Geográfica
GLONASS	Sistema Global de Navegación por Satélite (Rusia)
GNSS	Sistema Global de Navegación por Satélite
GPS	Global Positioning System (Sistema de Posicionamiento Global)
IR	Radiación Infrarroja
LSS	Low Slow Small
LWIR	Infrarrojos de longitud de onda larga
LWR	Laser Warning Reveiver
MIL-STD	Estándar Militar
MWIR	Infrarrojos de longitud de onda media
NBQR	Nuclear, Biológico, Químico y Radiológico
OTAN	Organización del Tratado del Atlántico Norte
OTM	On The Move (En movimiento)
PEXT	Prácticas externas
POI	Probability Of Intercept (Probabilidad de interceptación)
RCS	Radar Cross Section
RF	Radio Frecuencia
RPAS	Remotely Piloted Aircraft System (Sistemas Aéreos Tripulados de forma Remota)
STANAG	Standardization Agreement (Acuerdo de Normalización)
TFG	Trabajo de Fin de Grado
UAS	Unmanned Aircraft Systems (Sistemas de Aeronaves no Tripuladas)
UAV	Unmanned Aerial Vehicle (Vehículo Aéreo no Tripulado)

PÁGINA INTENCIONADAMENTE EN BLANCO

1. Introducción

Esta memoria presenta el Trabajo Fin de Grado titulado “Sistemas Anti-drones, Neutralización y Detección de drones”, que se comenzó a realizar durante las prácticas externas llevadas a cabo en la Compañía de Transmisiones del Batallón del Cuartel General de la Comandancia General de Melilla entre los meses de septiembre y octubre de 2021.

1.1. Antecedentes

La creciente utilización de drones con fines maliciosos y lucrativos supone un riesgo en las zonas urbanas y en las zonas aisladas como pueden ser las zonas de operaciones. En este TFG se ha planteado abordar la problemática derivada de esta amenaza buscando soluciones para detectar, perturbar y neutralizar a estos drones. Desafortunadamente, la creatividad humana no se limita a fines legales o constructivos. Los terroristas y criminales están demostrando ser innovadores también en el uso de drones.

A continuación, se citan algunos casos reportados con drones hostiles, maliciosos y negligentes que han ocurrido durante los últimos años:

- Ejemplos de casos de contrabando y transporte de drogas a través de fronteras. La policía española incautó en Málaga, en julio de 2021, el mayor dron conocido hasta la fecha, dedicado al transporte de droga. El dispositivo tenía una envergadura de casi 4,5 metros y disponía de una autonomía de vuelo de siete horas. La capacidad de carga era de 150 kilos que se utilizaba para el transporte de hachís y cocaína entre las costas de Marruecos y España. (El País, 2021)
- Ejemplos de episodios de invasión de la intimidad y espionaje. Se trata de la obtención de información, generalmente gráfica (fotografía o video) de carácter privado (Aguilera, 2019).
- Ejemplos de episodios de disrupción del espacio aéreo en aeropuertos: el 18 y 19 de diciembre de 2018, aproximadamente 1.000 vuelos fueron cancelados en el aeropuerto de Gatwick (Inglaterra) por el avistamiento de drones no colaborativos cerca de la pista. Los dos sospechosos fueron liberados sin cargos. Por otro lado, el 9 de agosto de 2019, el Aeropuerto Internacional de *Abha* (Arabia Saudita) fue objeto de un ataque terrorista con drones a cargo de los rebeldes *hutíes* (Guillén, 2019).
- Ataques contra infraestructuras críticas: el 14 de septiembre de 2019, se reportó un ataque con drones contra una refinería y un campo de petróleo de la compañía saudí Aramco, lo que desestabilizó la producción, en un país desde el que se exporta el cinco por ciento del crudo que se consume en todo el mundo (Guillén, 2019).
- Por otro lado, tras las acusaciones de Estados Unidos y Gran Bretaña se sospecha que en julio de 2021 Irán atacó con al menos un dron a un buque en las costas de Omán. Este incidente tuvo como consecuencia la muerte de dos miembros de la tripulación y causó además una gran tensión en Oriente Medio. (Levy, 2021)

De la información obtenida de las entrevistas realizadas a expertos y que pueden ser consultadas en los Anexos 1, 2, 3, 4 y 5, los sistemas actuales en nuestras Fuerzas Amadas, son los siguientes:

- Sistema *AUDS* de Blighter: desplegado en Irak.
- Antidrones portátiles *DroneDefender* de la empresa americana Battelle: en buques de la Armada.
- Sistema *ARMS* de la compañía Indra: desplegado en Mali por el Ejército del Aire.
- Sistema *CERVUS* de la compañía Gradiant: desplegado en el REW31 del Ejército de Tierra.
- Sistema *Aeroscope* de DJI: integrado en otros sistemas para la detección de drones de este fabricante.

1.2. Objetivos y alcance

El objetivo principal de este TFG es realizar un estudio sobre los de sistemas de defensa contra drones de pequeño tamaño, que vuelan a baja altura y velocidad (C-UAS LSS), en instalaciones militares fijas, tanto en zonas urbanas como aisladas.

Los objetivos específicos de este TFG son los siguientes:

- Identificar la amenaza mediante el análisis del dron.
- Establecer el concepto operativo de las soluciones de sistemas anti-dron
- Llevar a cabo un análisis comparativo del estado del arte en cuanto a posibles sistemas anti-dron propuestos por diferentes empresas de reconocido prestigio del sector.
- Seleccionar los sistemas anti-dron más apropiados, adaptados al escenario elegido, para integrarlos en nuestras actuales Fuerzas Armadas y con la suficiente capacidad de proyección evolutiva para su integración en la futura Fuerza 35.

El alcance del TFG abarca la clasificación de la amenaza que presenta el uso malicioso de drones actualmente, en particular los UAS LSS, al situarse éstos fuera de los sistemas de defensa aérea actuales y, por tanto, de los sistemas de neutralización cinéticos tradicionales.

A este respecto se revisarán aquellos tipos de situaciones en los que pueden intervenir UAS. Este TFG incorporará también la selección de las posibles soluciones de sistemas anti-dron para los actuales problemas derivados del uso de UAS, así como la mejor opción para su utilización en las Fuerzas Armadas y en un futuro escenario de defensa de la Fuerza 35.

1.3. Ámbito de aplicación

En el presente trabajo se realizará el estudio los sistemas anti-dron basados en el ciclo de funcionamiento común: detección, identificación, decisión y neutralización. Será de aplicación tanto para las actuales Fuerzas Armadas como para la Fuerza 35, unidad que estará operativa en el año 2035 y que incorporará tecnologías emergentes y disruptivas que permitirá operar con mayor rapidez. Este nuevo modelo de Fuerza contiene una incorporación de medios tecnológicos avanzados en las estructuras orgánicas en el caso de inteligencia, drones y sistemas anti dron para posibles amenazas que se puedan presentar en el futuro.

Será también de utilidad, el presente estudio, en el ámbito de unidades operativas de la Guardia Civil y del Cuerpo Nacional de Policía, ya que la actividad policial en ese terreno crece al mismo ritmo que se produce la proliferación del uso de estas aeronaves. Se hace necesario el control del espacio aéreo de las ciudades. Es habitual detectar multitud de vuelos ilegales de estos dispositivos, incluso, en ocasiones, en las inmediaciones de espacios sensibles, como edificios públicos, hoteles, eventos multitudinarios, etc.

2. Metodología

Las herramientas más relevantes a utilizar para alcanzar los objetivos de este proyecto son las siguientes:

2.1. Revisión bibliográfica

En primer lugar, se revisará el uso de diversos tipos de drones en misiones específicas en la que se han utilizado como fuentes bibliográficas: artículos de revistas entre las cuales se incluye la revista Cuadernos de Gobierno y Administración Pública o la Revista Española de Derecho Internacional, informes del Ministerio de Defensa como el Concepto Nacional C-UAS LSS (*Counter Unmanned Aerial Systems Low Slow Small*), libros y manuales de tecnología militar, páginas web y artículos de prensa.

En segundo lugar, se realizará un análisis de diferentes tipos de sistemas anti-dron, obteniendo información, sobre todo, de las páginas web y artículos técnicos de los sistemas indicados por los expertos en las entrevistas realizadas.

2.2. Entrevista a expertos

El estudio sobre la sensibilidad y los posibles riesgos asociados a las amenazas que un mal uso de los drones pueda causar en entornos militares y civiles, además de diversos aspectos técnicos, se ha llevado a cabo en base a la información recapitulada, mediante entrevistas, realizadas al director de Indra en esta disciplina, a personal de dos unidades directamente ligadas a la amenaza de estos dispositivos y a personal de la Unidad donde se realizaron las prácticas externas (PEXT). Durante este tiempo, se ha podido tratar el tema con profundidad, obteniendo información sobre algunas capacidades de las que disponen nuestras Fuerzas Armadas para identificación y neutralización de drones que supongan alguna amenaza.

Se han materializado 5 entrevistas. El personal seleccionado se estableció atendiendo a las funciones atribuidas tanto en la empresa civil, como es el caso del director de Indra, como en las unidades de destino, para el resto de entrevistados militares, eligiendo aquéllas en las que se trabaja a diario en la detección de la amenaza que suponen los drones. El personal entrevistado fue el siguiente:

- D. Francisco Vázquez Vázquez, Director de Desarrollo de Productos de Defensa y Vigilancia Electrónica de Indra
- Tte. D. Alberto Bermejo Vesga, Jefe de Sección en la 11ª Batería 35/90 Skydor del Grupo de Artillería Antiaérea I/71.
- Brigada D. Ricardo Rodríguez Baña, Integrante de la Sección de Estudios y Proyectos del CCAL del Regimiento de Guerra Electrónica 31.
- Brigada integrante del Centro de Integración y Difusión de Inteligencia en COMGEMEL.
- Subteniente integrante del Centro de Integración y Difusión de Inteligencia en COMGEMEL.

El propósito de las mismas ha sido obtener información sobre la amenaza que supone la proliferación de drones en el ámbito militar y las medidas anti-dron que se están utilizado en la actualidad. Se puede decir, a modo de conclusión que:

- El Ejército es plenamente consciente de la amenaza de los drones.
- Se dispone actualmente de sistemas anti-dron para la detección y neutralización de drones, aunque es necesario la adquisición de un mayor número de estos sistemas.
- Se considera necesario que en todas las zonas de operaciones donde están desplegadas las fuerzas españolas, se dispongan de sistemas anti-dron.
- Se debe formar al personal para conseguir la especialización en este tipo de sistemas.
- Los sistemas anti-dron se deben ir actualizando constantemente según avanzan los medios tecnológicos.

En los ANEXOS 1, 2, 3, 4 y 5 se desarrollan las entrevistas realizadas.

2.3. Investigación comparativa de las soluciones tecnológicas anti-dron del mercado

En primer lugar, se efectuará un análisis DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades), mediante el que se valorará si resulta adecuado dotar de sistemas anti-dron a instalaciones militares fijas (bases aéreas, navales y terrestres), para su protección, en zonas urbanas y aisladas. Se ha elegido este tipo de análisis por tratarse de una herramienta adecuada para poner de relieve la realidad de un producto, para poder tomar decisiones de futuro. En este caso se analizará la oportunidad de proceder a la adquisición del sistema C-UAS.

Si bien el ejército dispone ya de estos sistemas, es de forma escasa y sólo para situaciones puntuales. Además, en la publicación "Concepto Nacional C-UAS LSS" (Defensa Gob, Estado Mayor de la Defensa, 2019), se presentó como propuesta de Problema Militar Operativo la carencia en las FAS de "*…una capacidad integral que permita prevenir, detectar, identificar, decidir y, en su caso, neutralizar los UAS LSS…*"

En segundo lugar, mediante análisis multicriterio (AMO), se realizará un estudio de las posibles soluciones propuestas por diferentes empresas de reconocido prestigio del sector. Se utiliza el análisis multicriterio, por tratarse de un instrumento que permite evaluar las posibles soluciones a un determinado problema, de acuerdo a diferentes criterios. Se trata de determinar la solución más conveniente que consiga un compromiso de satisfacción, en cuanto a los diferentes criterios evaluados. Se buscará en el caso que se está tratando, el tipo de sistema anti-dron más adecuado al escenario elegido.

3. Revisión bibliográfica

3.1. Análisis del dron

El fuerte incremento del mercado de los “drones” hace que exista una enorme variedad de tipos accesibles que pueden ser empleados por cualquier usuario y con muy diferentes fines.

Antes de considerar un concepto operativo y una solución de sistema anti-dron, parece conveniente tratar de parametrizar o tipificar los diferentes aspectos que, de un modo u otro, pueden condicionar la adopción de decisiones de selección de los sistemas.

A la hora de definir las amenazas a las que debe enfrentarse un sistema de neutralización de drones, es necesario, por tanto, acudir a diferentes criterios de clasificación, en tanto que van a condicionar las necesidades operativas a las que ha de atender el sistema. Entre estos criterios de clasificación están:

- Tamaño del dron
- Propósito del dron
- Entorno y localización del dron
- Guiado del dron

Este conjunto de parámetros va a condicionar la configuración de los sistemas anti-dron en todos sus aspectos, ya que de ellos van a depender los requisitos de detección, seguimiento e identificación, pero, sobre todo, va a condicionar las características de la reacción, ya sea ésta la inhibición, la neutralización o la destrucción. (Thales, 2019)

3.1.1. Tamaño del dron

El tamaño del dron va a condicionar fundamentalmente el tiempo de reacción frente a la amenaza que representa, así como la peligrosidad de la misma.

En la figura 1 se muestra la clasificación que establece la OTAN diferenciando tres tipos de dispositivos diferentes, según el peso, su alcance y altitud. (DEGAM, 2016)

En la clase I se incluyen los drones micro con pesos inferiores a 2 kg, los mini que se encuentran entre 2 y 20 kg y los small que están por encima de 20 kg y por debajo de 150 kg. La clase II comprende aeronaves con pesos comprendidos entre 150 kg y 600 kg y la clase III que contiene aquéllos con peso superior a 600 kg.

Los de menor tamaño (menos de 20 kg) habitualmente son drones civiles y los de tamaño medio y grande (más de 20 Kg), son generalmente militares, aunque también podemos encontrar drones civiles en este rango.

Class	Category	Normal employment	Normal Operating Altitude	Normal Mission Radius
CLASS I (less than 150 kg)	SMALL >20 KG	Tactical Unit (employs launch system)	Up to 5K ft AGL	50 km (LOS)
	MINI 2-20 kg	Tactical Sub-unit (manual launch)	Up to 3K ft AGL	25 km (LOS)
	MICRO <2 kg	Tactical PI, Sect, Individual (single operator)	Up to 200 ft AGL	5 km (LOS)
CLASS II (150 kg to 600 kg)	TACTICAL	Tactical Formation	Up to 10,000 ft AGL	200 km (LOS)
CLASS III (more than 600 kg)	Strike/ Combat	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)
	MALE	Operational/theater	Up to 45,000 ft MSL	Unlimited (BLOS)

Figura 1. Clasificación de drones según su tamaño. Fuente OTAN

Atendiendo al tipo de “dron amenaza” fijado en el objetivo

principal del presente estudio (UAS LSS), se describen a continuación los drones de los tipos micro y mini incluidos en la clase I. (Defensa Gob, Estado Mayor de la Defensa, 2019)

– **Drones micro clase I (peso menor de 2 kg)**

El alcance de detección para dispositivos de estos tamaños se estima en 4 km. Este tipo de drones comerciales son las amenazas de menor tamaño a neutralizar por los sistemas anti-dron. Son baratos y de fácil disponibilidad. Las figuras 2, 3 y 4 muestran drones de este tipo, de diferentes fabricantes.

Figura 2. Automn drone. Fuente: Indra

Se trata de drones con un coste de 300€ a 1000€ con capacidades limitadas en cuanto a control y a carga útil, aunque cada vez son más sofisticados, tendencia que se mantendrá e incrementará con toda probabilidad. (Blázquez García, 2018)

Figura 3. Dron Skywalker X8. Fuente: Indra

Envergadura 2122mm; Peso 880 g; Superficie del ala 80 dm2.

Estos tipos de drones se caracterizan por:

- Disponibilidad y precio asequibles.
- Baja letalidad.
- Capacidades limitadas (cargas útiles por debajo de 500 gr).
- Bajo tiempo de reacción. Si consideramos la detección de un micro-dron a una distancia de 1 km, con una velocidad de vuelo de 20 m/s (velocidad máxima del modelo DJI *Phantom* 4), se dispondrían escasamente de 50 s para su neutralización.
- Tiempo de misión corto. La autonomía característica de estos dispositivos es de unos 20 minutos, suponiendo plena carga de las baterías, lo que, no obstante, les confiere una distancia de acción de varios kilómetros. (AESA, 2019).

Figura 4. Dron DJI Phanton 3 Fuente: Indra

STANDARD Tamaño Diagonal 350mm Peso 1216g.

– **Drones mini clase I (peso entre 2 kg y 20 kg)**

Los drones mini tienen una capacidad de carga de hasta 15 kg. La figura 4 muestra un ejemplo de dron diseñado para portar cargas útiles pesadas. El HYDRA tiene 12 motores, lo que le permite transportar hasta 12 Kg (26.5 lbs) de carga útil efectiva (Onyxstar , 2022)

Figura 5. Dron multicóptero Hydra-12. Fuente: Directindustry

Este tipo de drones están caracterizados por:

- Precio menos asequible (>15k€).
- Posible letalidad media/alta.
- Cargas útiles de hasta 15 kg.
- Mayor tiempo de reacción, ya que pueden ser detectados a mayor distancia.
- Posibilidad de misiones más largas con el uso de baterías suplementarias sacrificando parte de la carga útil.

- Velocidad de crucero de vuelo de hasta 15 km/h.

(Onyxstar , 2022)

3.1.2. Propósito del dron

El propósito de la amenaza guarda relación con el modo de operar esperable y con las medidas de reacción necesarias.

El uso de drones con objetivos irregulares o ilegales está relacionado con actividades muy diversas:

- Transporte de droga: una cámara de seguridad grabó en mayo de 2016 a un dron en el momento de entregar un paquete con drogas y teléfonos móviles en una celda de la prisión de Wandsworth en Londres. (BBC, 2016)
- Ataque a aviones civiles: en Reino Unido, el aeropuerto de Heathrow, en Londres, el vuelo de la aerolínea British Airways procedente de Ginebra, con 132 pasajeros y tripulación de cinco personas, fue golpeado por un dron cuando se aproximaba a la capital de Inglaterra. (BBC, 2016)
- Intención de causar daño mediante el uso de explosivos: un dron cargado de explosivos lanzado desde la Franja de Gaza fue derribado por un avión de combate F-16 israelí. El dron, denominado “suicida” transportaba cinco kilogramos de explosivos. (Zona Militar, 2021)
- Contrabando de drogas a través de las fronteras: utilización de drones para traficar droga a través de la frontera en México. (BBC, 2015)
- Portadores de armas de destrucción masiva: en el año 2002 Al Qaeda planeó lanzar un dron repleto de ántrax en soporte gaseoso para atacar la Cámara de los Comunes británica. (Global Estrategy, 2020)
- Atentados selectivos: Al-Qaeda en 2001, planeó un ataque con pequeños artefactos explosivos improvisados (IEDs) que portarían drones, contra el presidente George W. Bush y demás líderes internacionales en la convención del G8 en Génova, Italia. (Global Estrategy, 2020)

Desde el punto de vista del modo de operación, podemos organizar el uso de los drones de acuerdo al número de ellos que participan en el ataque:

- Individual: resulta la amenaza más simple, ya se trate de drones espía, contrabando o cualquier otra amenaza de mayor letalidad.
- Colectiva o de enjambre: debido a la disponibilidad de drones baratos, es normal pensar en la posibilidad de activar distintas oleadas de drones, siendo algunos de ellos amenazas reales o simples señuelos. De cualquier forma, los ataques en enjambre dificultan el seguimiento y la neutralización.
  (Defensa Gob, Estado Mayor de la Defensa, 2019)

3.1.3. Entorno y localización del dron

Por un lado, el lugar en el que se produce la amenaza va a alterar los medios técnicos que se utilicen tanto para la detección y seguimiento como para la neutralización.

La detección y neutralización en **zonas urbanas** será tanto más compleja cuanto mayor sea la densidad de población en la zona y más heterogénea la arquitectura urbana. La presencia de amenazas en zonas públicas y pobladas dificultará posiblemente su detección y seguimiento por la presencia de obstáculos (edificios, árboles, etc), favoreciendo incluso estrategias de acercamiento al blanco utilizando las zonas ciegas de los sensores.

En este aspecto hay que considerar como un factor adicional la regulación actual o futura del vuelo de los drones. Parte de los espacios públicos (especialmente en área urbana) están prohibidos

para estos aparatos, por lo que la detección de la presencia de uno de ellos lo convierte directamente en una amenaza. Igualmente, en este tipo de entornos urbanos, o poblados, las medidas de neutralización han de ser especialmente cuidadosas.

Por otro lado, en el extremo contrario, se sitúan infraestructuras localizadas en **zonas aisladas** y alejados de núcleos urbanos en los que las posibilidades de detección a gran distancia son factibles y las posibilidades de utilizar cualquier tipo de contramedida son, a priori, aceptables.

Hay que atender a la propia tipología y vulnerabilidad de la infraestructura a proteger. En este sentido, la protección de un palacio (Moncloa, Zarzuela, por ejemplo) o la protección de una central nuclear necesitarán de una serie de soluciones *ad hoc*, ya que sus vulnerabilidades son completamente diferentes.

Una vez diferenciadas las dos zonas de actuación de los UAS, podemos establecer los siguientes entornos de protección:

Entornos civiles: en los que se incluyen centrales nucleares y aeropuertos, cárceles, tráfico de drogas en fronteras y aglomeraciones en diferentes acontecimientos públicos.

Entornos militares: incluyendo bases aéreas, navales y terrestres, zona de operaciones, buques, almacenes de armas y explosivos.

(Defensa Gob, Estado Mayor de la Defensa, 2019)

3.1.4. Guiado del dron

El mercado actual de drones comerciales (sin considerar el ámbito militar) incluye diferentes tipos de guiado:

- Guiado manual mediante el enlace de control. Un operador controla el vuelo del dron remotamente recibiendo imágenes de las cámaras del propio dron, así como datos de su posición via radio-enlace, y envía comandos por la radio de control, conduciendo el dron manualmente a través de un “joystick”.
- Guiado mediante waypoints (GPS). Se define la trayectoria que debe seguir el dron hasta su destino, en forma poligonal, definiendo puntos por donde debe pasar. Apoyado en la información que le da el GPS permite un vuelo automático, preprogramado mediante esos “waypoints”
- Guiado inercial. Guiado automático similar al anterior pero, en este caso, la posición en cada momento del vuelo se obtiene de sensores inerciales instalados en el dron (giróscopos, acelerómetros, brújula, altímetros, etc.) en lugar del GPS.
- Guiado por reconocimiento de imagen. Con imágenes previamente grabadas del terrero, por ejemplo, obtenidas desde satélites, al dron se le programa una trayectoria como sucesión de imágenes a seguir. Va comparando la imagen de su cámara con la almacenada previamente en la definición de su trayectoria para seguirla. También se usa esta técnica para el aterrizaje de vuelta a casa, donde el propio dron fotografía el punto de despegue y lo guarda en su memoria, para después utilizarlo en el aterrizaje con precisión en el mismo punto de despegue.

Aunque en principio es difícil determinar el modo de guiado de un dron, se puede obtener información del mismo mediante:

- La detección de señales de RF (Radio Frecuencia) en las bandas de telecontrol, aunque es cierto que una pequeña manipulación de equipos comerciales, puede permitir mover los canales de control a frecuencias diferentes a las reguladas para este tipo de uso (27/49/50/53/72/75 MHz y 2,4GHz).
- La disponibilidad de una base de datos de modelos y comportamientos asociados, puede facilitar la toma de decisiones asociada a las contramedidas. Cada modelo de los disponibles en el mercado, tiene un comportamiento predecible en presencia de diferentes perturbaciones a sus canales de control o a la señal GPS (Sistema de

Posicionamiento Global). La reacción de un dron frente a una perturbación puede permitir identificar el modelo y, en sentido contrario, la identificación (firma doppler o imagen, p. ej.) del modelo, puede permitir seleccionar la contramedida más adecuada. (Gavilán Jiménez, 2012), (Defensa Gob, Estado Mayor de la Defensa, 2019).

3.2. Concepto operativo de las soluciones de los sistemas anti-dron

Resulta complicado establecer un perfil único para definir la Misión de un Sistema Anti-Dron y, por tanto, sus conceptos operativos.

Los drones, por su versatilidad, accesibilidad y facilidad de uso, representan un concepto de innumerables aplicaciones tanto en un lado como en el otro de un conflicto de intereses.

No obstante, establecido el contexto, centraremos el análisis en el campo de las aplicaciones de la Defensa y de la Seguridad Ciudadana.

En este contexto abordaremos el análisis de los conceptos operativos desde una óptica clásica que cubre las siguientes fases:

- Vigilancia y Conciencia Situacional
- Mando, Control y ayuda a la decisión
- Reacción

(Defensa Gob, Estado Mayor de la Defensa, 2019)

3.2.1. Operación de vigilancia

Los elementos sensores que, a priori, serían de aplicación para este tipo de escenarios son adaptaciones de los clásicos de vigilancia de espacios aéreos (Defensa Gob, Estado Mayor de la Defensa, 2019)

- Sensores radar: proporcionan conciencia situacional global
- Sensores ópticos y optrónicos: proporcionan capacidad de confirmación e identificación
- Sensores acústicos: proporcionan conciencia situacional cercana
- Sensores de comunicaciones: proporcionan conciencia situacional radioeléctrica
- Sensores colaborativos: complementan la funcionalidad de confirmación e identificación

La funcionalidad de estos sensores condiciona la selección de los mismo para su aplicación. Así, las características específicas de capacidad de detección, falsa alarma y entorno de vigilancia de estos elementos, determinan en primer lugar que las tecnologías radar aplicables son aquellas capaces de lidiar con blancos imprevistos, en entornos de falsa alarma, de baja RCS (Radar Cross Section), o lo que es lo mismo, blancos de difícil detección y que se pueden confundir con elementos que no suponen amenaza. Asimismo, deben tener una alta capacidad de despliegue y autonomía de operación.

El radar es el sensor que es capaz de detectar los drones y de medir su posición en las 3 dimensiones del espacio, en el caso de radares 3D. Es decir, mide la distancia, el ángulo en azimut y el ángulo en elevación en el que se encuentran los drones, por lo que se puede neutralizar de forma selectiva. Es el sensor primario de detección y localización y por tanto da información de conciencia situacional de posición y global en el espacio 3D. Si el radar está basado en tecnología de detección Doppler, éste ofrecerá la posibilidad de clasificar los drones según su firma Doppler, para diferenciarlo de otras potenciales fuentes de falsas alarmas como pueden ser los pájaros.

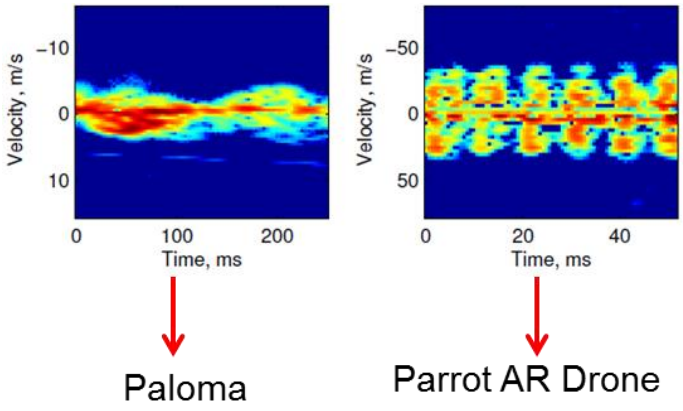

Figura 6. Clasificación según firma Doppler. Fuente: Indra

En la figura 6 se muestra la clasificación según la firma Doppler de una paloma y un UAS de uso recreativo civil Parrot AR Drone.

Los sensores ópticos y optrónicos representan un elemento fundamental dentro de la función de identificación. Para ello se consideran todos los espectros de operación en que estos elementos puedan ser detectados. Desde el espectro visible hasta el térmico infrarrojo en todas sus bandas de operación. No es descartable la incorporación, dentro de esta gama de sensores, los detectores láser (LWR, Laser Warning Reveiver) como elemento adicional de protección de puntos críticos, ante designadores o telémetros que puedan ser portados desde un dron, en apoyo a la operación de otros elementos externos.

Respecto a estos sensores ópticos optrónicos, los condicionantes de tamaño y entorno, hacen que sea necesario establecer ciertos condicionantes para que estos no interfieran a los sensores radar y acústicos analizados anteriormente. Los sensores ópticos utilizados deben tener alta sensibilidad (baja radiancia de los elementos a detectar), unido a alta precisión (pequeño tamaño y alta capacidad de mimetización). Por tanto, deben ser elementos muy directivos con una gran precisión de apuntamiento que, en lo esencial, debe ser determinada por el dato radar por lo que debe tener alta precisión de determinación de posición de los blancos. Aquí entra en juego el dato 3D como altamente deseable para el dato radar.

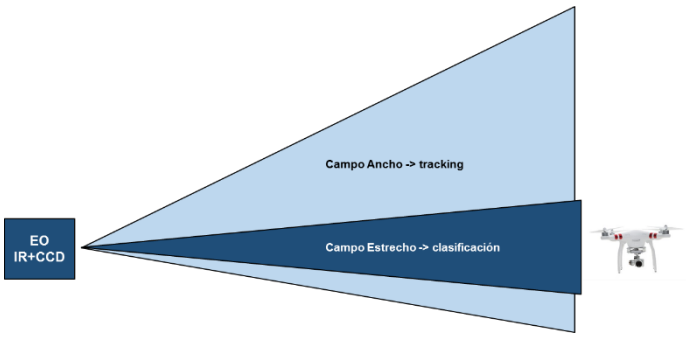

Figura 7. Campos de trabajo de cámara infrarroja y visible. Fuente: Indra

En la figura 7 se indican los diferentes ángulos de campo de la cámara de infrarrojo y visible EO/IR, para las operaciones de tracking y clasificación.

En la figura 8, se muestra el modo vigilancia. El radar detecta y localiza con su ancho de haz estrecho. El sensor IR hace tracking-seguimiento con el FOV ancho y conmuta a FOV estrecho para la identificación, reconocimiento y clasificación.

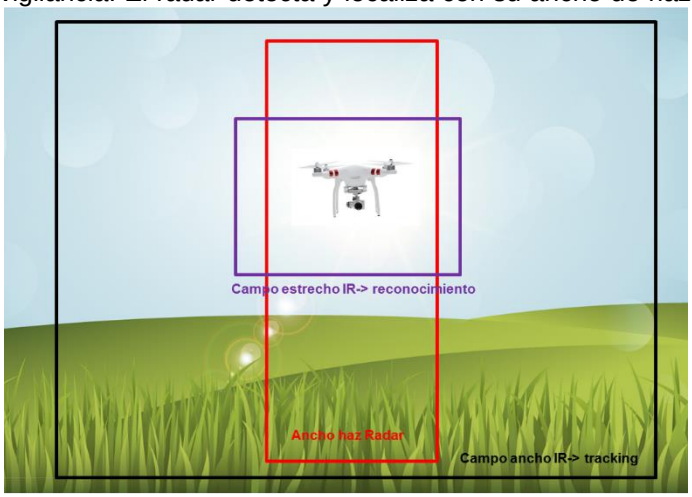

Figura 8. Modo vigilancia del sistema anti-dron. Fuente: Indra

En cuanto a los sensores acústicos, se debe definir su aplicación atendiendo a la frecuente operación de los sistemas de detección en escenarios extraordinariamente ruidosos (afluencia masiva de gente, entornos urbanos, etc.). Sin embargo, son elementos de detección de rango cercano no descartables a priori si su operación se centra en espectros de sonido muy particulares y definitorios de la operación del dron y muy diferenciales respecto al entorno.

En cuanto a los sensores de comunicaciones, los drones son fuentes de transmisión de señales radioeléctricas tanto de datos como de monitorización y control. Sin embargo, dicha transmisión de datos suele ser directiva y, por tanto, difícil de detectar. Los sensores de comunicaciones detectan los enlaces radio que hay entre el dron y el piloto (enlaces de datos y enlaces de control), de forma que define la frecuencia y características de los enlaces radioeléctricos o de radiofrecuencia que emiten el dron y/o la estación de control del dron en tierra, para poder neutralizarlos con perturbación (jamming). También, mide el ángulo donde se encuentran el dron y la estación de control, por lo que da información de conciencia situacional desde el punto de vista de detección de señales de radio. la complejidad de las señales a detectar, así como los niveles de sensibilidad requeridos, hacen que este tipo de sensores deban ser relativamente capaces y sofisticados lo que, frecuentemente, limita su desplegabilidad y restringe su uso para entornos de operación muy concretos.

Por último, los sensores colaborativos no permiten realmente contribuir a la conciencia situacional primaria, pero la complementan con información que permite optimizar la función de identificación, por cuanto descarta blancos presentes, pero no de interés desde el punto de vista de detección de amenazas. Complementan la funcionalidad de confirmación e identificación mediante la integración y fusión de información procedente de varios tipos de sensores (radar, cámaras, radiogoniómetros, etc). Se mejora de esta forma la identificación y localización del dron objetivo del sistema anti-dron. Este tipo de sensorización, establece un entorno de información de elementos en vuelo no amenazantes, como puede ser un ave, que se puede llevar a cabo por identificadores detectables en los elementos en vuelo (balizas), o mediante integración en la capa de mando y control de datos procedentes de las estaciones de control de dichos elementos en vuelo, con datos de posición de los mismos en tiempo real. (Thales, 2020), (Isdefe, 2016-2017) (Indra, Indracompany, 2021).

En la figura 9, se muestra un diagrama de lo que podría ser un sistema anti-dron. Como sensor primario se representa un radar 2D. Como sensores secundarios se representan: de infrarrojo, de detección RF y de audio. A continuación, se muestra el módulo de fusión y toma de decisión de los sensores, y finalmente la ejecución de contramedidas, que podrán realizarse por orden de operador o de forma automática.

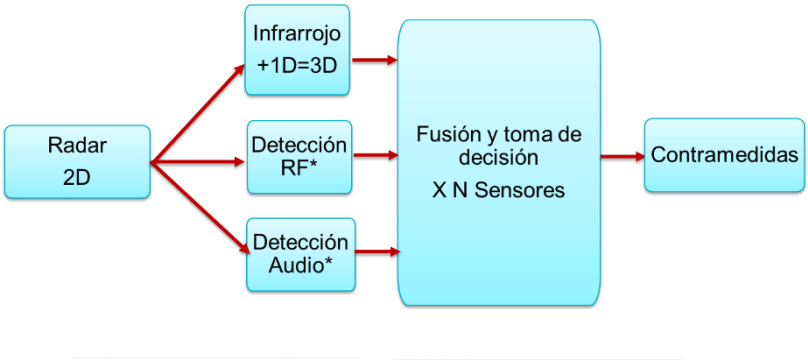

Figura 9. Sistema anti-dron. Fuente: Indra

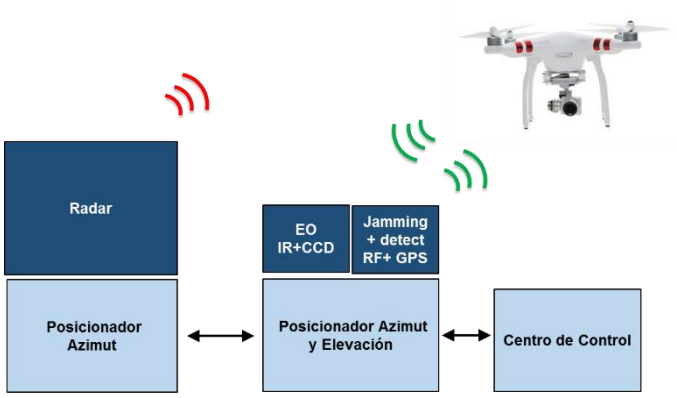

Figura 10. Sistema anti-dron. Fuente: Indra

En la figura 10, se muestra otra representación de sistema anti-dron. Mediante radar y cámara visible y de infrarrojo EO/IR, se establece la distancia, Azimut y Elevación. Se utiliza, en este caso, *Jamming* e inhibición de GPS como medida de neutralización del dron.

Los conceptos operativos a tener en cuenta dentro del escenario de Vigilancia y Conciencia Situacional son, entre otros, los siguientes:

- Baja detectabilidad
  - Potencial pequeño tamaño
  - Uso de elementos compuestos de baja RCS
  - Falta de predictibilidad o preaviso por rango de actuación corto
  - Baja huella sonora
- Entorno de probable falsa alarma
  - Comportamiento asimilable al de otros elementos (aves, etc.)
  - Integración en escenarios con otros elementos similares no amenazantes
  - Entorno legal difuso que dificulta la catalogación como elementos amenazantes
- Entorno complejo
  - Necesidad de establecer perímetros de vigilancia *ad hoc*
  - Necesidad de desplazar y desplegar elementos de vigilancia
  - Dificultad para establecer la infraestructura del despliegue de sensores

Derivado del análisis anterior, se establecen como características específicas para la elección de los elementos de vigilancia y conciencia situacional los siguientes:

- Radar: aplicación de radares de baja potencia de transmisión y con alta capacidad de

procesado de la información obtenida de los blancos (rotores, aspas, etc.). Alta precisión en la determinación de la posición de los blancos. Es deseable para la optimización de la función óptica, la capacidad de dato 3D de los sensores radar. Deben tener una alta desplegabilidad, y la mayor autonomía posible para tener versatilidad de operación.

- Sensores acústicos: se consideran un elemento deseable de valor añadido, pero no prioritarios. Deben tener capacidad de operación en espectros específicos que le permitan operar en entornos ruidosos, además de un elevado margen dinámico que impida su saturación por ruido cercano. No en todas las aplicaciones de seguridad son de la misma utilidad, pero hay entornos en los que estarían especialmente indicados como son los de control de fronteras conflictivas.
- Sensores ópticos y optrónicos: se considera de interés la utilización de sensores en espectro visible y de luz infrarroja. Deben tener ópticas de alcance compatible con la precisión de los datos radar y deben asentarse sobre posicionadores 3D, con precisión y velocidad de posicionamiento compatibles con la operación de tracking, o seguimiento automático de objetivos en secuencias de vídeo. Adicionalmente deben tener una resolución de imagen capaz de implementar funciones de tracking basadas en imagen, además de posibilitar la identificación/clasificación del dispositivo mediante zoom óptico de alta sensibilidad.

Figura 11. Imagen IR de ejemplo para tracking (seguimiento). Fuente: Indra

En la figura 11 se muestra imagen IR utilizada por el sistema anti-dron para la operación de tracking.

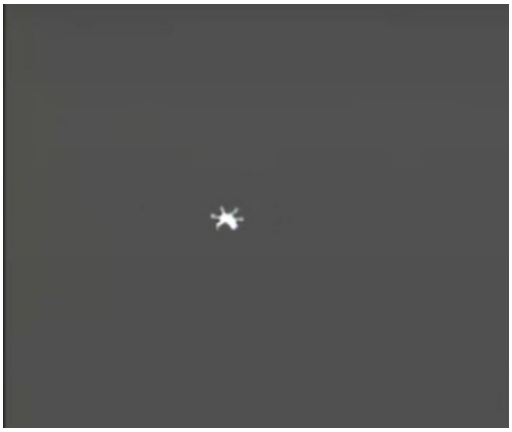

Figura 12. Imagen IR de ejemplo para clasificación. Fuente: Indra

En la figura 12 se muestra imagen IR utilizada para identificación/clasificación. Se puede observar una resolución mejorada, mediante la ampliación con zoom óptico, respecto a la imagen anterior.

Cuantos más sensores de este tipo se dispongan, en diferentes localizaciones, con mayor precisión se podrá determinar la posición del dron, mediante triangulación, o cualquier otra técnica telemétrica. De esta forma se puede designar como blanco, al dron amenaza para su interceptación y derribo.

- Sensores de comunicaciones: radiogoniómetros específicos para detectar la dirección de

procedencia de las señales de radio, tanto de control de vuelo como de transmisión de datos.

- Sensores colaborativos: se considera un elemento no exigible ya que condiciona fuertemente el escenario y resulta de difícil implementación, sin garantizar la correcta identificación del escenario amenazante.

(Isdefe, 2016-2017) (Indra, Indracompany, 2021).

3.2.2. Mando y control y ayuda a la decisión

Los elementos funcionales que, a priori, serían de aplicación para este tipo de escenarios son: (Defensa Gob, Estado Mayor de la Defensa, 2019)

- Función de Fusión Multi-Sensor
- Función GIS (Sistema de Información Geográfica)
- Función Identificación
- Función de Supervisión
- Integración de Escalón Superior

La Función de **Fusión Multi-sensor** representa una de las funciones clave dentro del establecimiento de la Conciencia Situacional. Es responsabilidad primaria de esta función la fusión óptima de sensores de un despliegue fijo, semimóvil o táctico, que debe integrar redes de múltiples sensores del mismo tipo, así como también integración entre redes de sensores de diferentes tipos. La integración multisensor debe aportar a la función no sólo la evidente mejora en la calidad del dato, sino también un sensible incremento en la probabilidad de interceptación.

En cuanto a la **Función de Identificación**, en este caso es una función fuertemente vinculada con la de Fusión. Dentro de esta función, deben estar incorporados todos los algoritmos de funcionamiento colaborativo multisensor, así como los datos complementarios procedentes de otras agencias y sistemas de operación. Adicionalmente, una parte esencial de esta función es la de utilidades de procesado y mejora de imagen, gestión de imágenes superpuestas y gestión de Bases de Datos de elementos inventariados.

En cuanto a la **Función GIS** (Sistema de Información Geográfica) es una herramienta para trabajar con información georreferenciada. La información georreferenciada es aquélla que viene acompañada de una posición geográfica.

La Función GIS debe, asimismo, incorporar requisitos específicos de la operación anti-dron. A las funciones GIS clásicas resulta conveniente, en muchas aplicaciones de seguridad, la incorporación de datos de entorno urbano.

Una función auxiliar, pero de vital importancia es la **Función de Supervisión**. Ésta incorpora todas las herramientas orientadas a la monitorización permanente de los elementos asociados al Sistema, diagnóstico de su estado de operatividad y toma de decisiones automáticas, semi-automáticas o manuales, en función del indicado estado de operatividad. Debe permitir la identificación precisa del elemento en fallo, así como aportar información sobre el nivel de operatividad o degradación en presencia de dicho fallo.

Por último, la **Función de Integración** en escalón superior, representa la adaptación de la capa de Mando y Control a la doctrina de organización y toma de decisiones de la operación. Resulta de especial relevancia cuando de lo que se trata es de un despliegue táctico, con una subordinación a un Mando Central o Centro de Gestión de Emergencias. (Indra, ARMS Sistema Multisensor, 2019), (Indra, Indracompany, 2021)

3.2.3. Reacción

Este concepto operativo debe permitir comandar diferentes perfiles de actuación, tanto en perfil *SoftKill* (se basa en la técnica *jamming* y *spoofing*) como *HardKill*. Como factor diferencial, dentro de misiones *HardKill*, se considera el comando de drones de interceptación e inutilización por colisión, en operaciones comandadas por la capacidad de tracking (seguimiento) de la función de

identificación.

Así, es necesario definir perfiles y parámetros de misiones *SoftKill*, donde el dron es interceptado y capturado a través del condicionamiento de su comportamiento por interferencia en sus sistemas de control, o de *HardKill*, en las que el dron es interceptado e inutilizado por algún medio destructivo. En ambos casos, deberán gestionarse diferentes sub perfiles de misión, de los cuales se extractan algunos, a continuación, a modo de ejemplo:

- *SoftKill*, medidas no destructivas empleando interferencias infrarrojas para bloquear los enlaces de comunicación del Dron.
  - Perfiles de *Jamming*, perturba la señal existente entre el operador y el dron.
  - Perfiles de *Spoofing*, "engaña" al sistema de posicionamiento vía satélite del dron (GPS, GLONASS, GALILEO), para desviarle de su trayectoria asignada.
- *HardKill*. puede producir daños colaterales a población civil o infraestructuras no militares.
  - Perfiles de derribo por *shooting* (disparando al dron mediante munición de fuego, por ejemplo)
  - Perfiles de derribo por operación de drones anti-dron
  - Perfiles de captura

(Thales, 2019)

En la figura 13 se muestra la actuación de un dron, mediante una red, para interceptar el dron hostil. Este dron de contramedida debería estar a cubierto y desplegarse bajo las órdenes del operador.

Figura 13. Hardkill. Fuente: Indra

Una vez descritos los modos de reacción *SoftKill* y *HardKill*, se establece a continuación cuándo están indicados, dependiendo del entorno de protección:

Entornos civiles: Se usarán preferentemente contramedidas ***Softkill***

- **Centrales nucleares y aeropuertos:** necesidad de sistemas con contramedidas que dispongan de antenas directivas, con zonas de exclusión para no causar perturbaciones en la función y operación normal de estas instalaciones. Los sistemas de detección serán de alta precisión en la medida del ángulo de llegada de los drones.
- **Cárceles (evitar introducción de drogas y armas)**: sistemas de bajo coste con contramedidas basadas en antenas omnidireccionales que cubren los 360 grados con una sola antena.
- **Tráfico de drogas en fronteras:** cobertura de grandes extensiones geográficas, obligan a instalar un conjunto de sistemas en red de gran alcance tanto en detección como contramedidas.
- **Aglomeraciones** en campos de futbol, plazas de toros, manifestaciones, etc. Sistemas ligeros y portátiles por policía o agente de seguridad, **tipo fusil**

Entornos militares: Contramedidas tanto ***Softkill*** como ***Hardkill***

- **Bases aéreas, navales y terrestres en zonas urbanas:** como en los entornos civiles, sólo se pueden usar contramedidas *Softkill*
- **Bases aéreas, navales y terrestres en entornos aislados:** posibilidad de usar además contramedidas *Hardkill*
- **Zona de operaciones y buques:** necesidad de sistemas móviles y portables
- **Almacenes de armas y explosivos:** necesidad de sistemas con contramedidas que

dispongan de antenas directivas, con zonas de exclusión para no causar perturbaciones en la función y operación normal de estas instalaciones. Los sistemas de detección serán de alta precisión en la medida del ángulo de llegada de los drones.

3.3. Soluciones de diferentes tipos de sistemas anti-dron

De la información obtenida de las entrevistas realizadas a expertos, tal y como se establecía en los antecedentes, los sistemas actuales en nuestras Fuerzas Amadas, son los siguientes:

- Sistema *AUDS* de Blighter: desplegado en Irak.
- Antidrones portátiles DroneDefender de la empresa americana Battelle: en buques de la Armada.
- Sistema *ARMS* de la compañía Indra: desplegado en Mali por el Ejército del Aire.
- Sistema *CERVUS* de la compañía Gradiant: desplegado en el REW31 del Ejército de Tierra.
- Sistema *Aeroscope* de DJI: integrada en otros sistemas para la detección de drones de este fabricante.

De la entrevista realizada al experto de Indra, se obtuvo la descripción básica del sistema anti-dron *ARMS*, diseñado por su empresa y, además, el conocimiento de los principales sistemas en el mercado, competidores directos del citado sistema de Indra. Los sistemas anti-dron referidos por el experto de Indra como adversarios comerciales del sistema *ARMS*, fueron los siguientes:

- *Horus Captor* de Grupo francés Thales
- *ADRIAN* de la empresa italiana Electrónica Roma
- *Leonidas* de la empresa Epirus estadounidense
- *Drone Guard* israelí de la empresa Elta System

Se analizarán a continuación los anteriores sistemas anti-dron, concluyendo mediante un análisis multicriterio, cual es el sistema que mejor se adapta al objetivo de protección de instalaciones fijas, tanto en zonas urbanas como aisladas. Cabe significar la dificultad encontrada en la obtención de información, al tratarse de una tecnología incipiente.

3.3.1. Sistema AUDS de Blighter

El sistema *AUDS* (Anti-UAV Defence System) dispone, para la neutralización de amenazas, de un inhibidor de radiofrecuencia con rango de interferencia que va desde 400 MHz hasta 6 GHz. Dispone de radar basado en tecnología de detección Doppler, cámaras electro-óptica EO y térmica para clasificación (tamaño del dron e identificación del modelo) que permiten hacer tracking, combinando la información aportada por estos sensores mediante fusión de éstos (fusión de sensores). Una vez clasificada la amenaza, el operador puede tomar la decisión adecuada con el sistema de mando y control. Como medidas de neutralización utiliza la inhibición GLONASS y la inhibición inteligente de RF que interfiere selectivamente las frecuencias requeridas hasta 6 GHz. Las antenas RF son direccionables, con alta directividad, para lograr el máximo rango de operación con el mínimo efecto colateral. El sistema puede ser utilizado en zonas urbanas y aisladas. Es modular y escalable.

Figura 14. Radar, cámara de video EO e inhibidor direccional RF. Fuente: Bligter

Transportable en plataformas.

El la figura 14 podemos observar los elementos de que consta el sistema *AUDS*. De izquierda a derecha:

- Radar: rango de detección: 10 km, de tecnología Doppler, cobertura de acimut: 180° (estándar) o 360° (opcional), ajuste de elevación: -40° a +30°.
- Cámara de vídeo electro-óptica EO y cámara térmica:
  - Cámara EO acimut: continuo, elevación: -50° a +60°, velocidad máxima: 60° por segundo, color HD 2.3 MP, zoom óptico: x30, zoom digital: x12, enfoque: automático.
  - Cámara térmica: resolución: 640 x 512 píxeles, zoom: 24° a 1,8° FOV.
- Inhibidor de RF direccional: antena de alta ganancia (6 GHz), incluye frecuencias GNSS, RF inteligente definida por software de inhibición

(Blighter, 2020)

3.3.2. Anti-dron portátil Dronedefender de Battelle

Este sistema anti-dron es portátil. Está pensado para protección de unidades en desplazamientos. Requiere siempre la intervención de un operador, que es el que detecta, identifica y toma la decisión de la neutralización mediante la inhibición. Tiene la ventaja de poder entrar en acción en un breve espacio de tiempo. El método de inhibición utilizado es *Jamming*, Se crean interferencias para inhabilitar los sistemas de telecontrol, comunicación y radionavegación del dron.

Figura 15. Fusil Dronedefender. Fuente: Battelle

El sistema se compone de un fusil (figura 15), con tres antenas inhibidoras de señal, baterías intercambiables y una mochila para su transporte. El funcionamiento consiste en apuntar al dron amenaza y accionar los disparadores disponibles. Monta dos disparadores, uno para inhibición de las comunicaciones y el otro para la perturbación de la señal GNSS. Se pueden accionar de forma independiente o ambos a la vez.

Las características incluyen:

- Tiempo de funcionamiento: 2 horas continuas de funcionamiento
- Peso: 6,8 kg
- Frecuencia de inhibición: 433MHz; 2,4 GHz y 5,8 GHz
- Alcance: 400 m
- Múltiples antenas

(Battelle, 2021)

3.3.3. Sistema ARMS de Indra

El sistema *ARMS* (Anti RPAS Multisensor System) está formado por sensores de distintas tecnologías para maximizar la probabilidad de detección, minimizar las falsas alarmas y usar las contramedidas de una manera eficaz.

El sistema dispone como sensor primario el radar que permite explorar varios kilómetros cuadrados en un segundo reportando la posición de la amenaza geográficamente (latitud, longitud), por lo que se puede determinar si se encuentra dentro del área a proteger.

Como sensor secundario principal dispone de un sistema optrónico con cámara térmica y cámara de espectro visible.

Incluye sensores de detección de radiofrecuencia y acústicos omnidireccionales y directivos que a su vez pueden funcionar como sensores principales siempre que tengan capacidad de exploración rápida.

La secuencia de detección estándar será la siguiente:

1. Detección y clasificación radar
2. Apuntamiento de sensores secundarios a la detección radar y análisis por parte de éstos
3. Fusión de datos de todos los sensores -> Alarma
4. Ejecución de contramedidas por orden de operador o automática

Las características principales del radar de detección son las siguientes:

- Radar basado en tecnología de detección Doppler
- Radar 3D
- Velocidad de rotación >= 60 RPM
- Rango de detección >= 1Km para drones de 0.01 m^2
- Cobertura de elevación >=12º ajustable mecánicamente en función del escenario.

El conjunto optrónico, mostrado en la figura 16, está compuesto por:

- Posicionador en azimut y elevación
- Cámara Térmica con FOV fijo similar a la cobertura de elevación del radar para seguimiento.
- Cámara Térmica con Zoom óptico continuo para clasificación
- Cámara visible con zoom óptico de alta sensibilidad para clasificación (identificación del dron).
- Procesamiento de imagen en formato RAW (formato de imagen sin pérdida de datos)

Figura 16. Conjunto optrónico sistema ARMS. Fuente: Indra

La detección RF se realiza mediante exploración de 360º con frecuencias de 27 MHz a 6 GHz. Radiogoniometría precisa en Tiempo Real.

La detección de audio se realiza mediante sensor de exploración de 360º.

El sistema de Mando y Control dispone de las funciones siguientes:

- Fusiona los datos de todos los sensores
- Software para determinación del tamaño del dron.
- Desencadena las contramedidas en caso de que sean necesarias, ya sea de forma automático o a petición del operador
- Muestra al operador las detecciones y alarmas de todos los sensores de una forma amigable.
- Representa los sensores y amenazas sobre GIS.
- Graba y reproduce eventos/video.
- Modular y escalable.
- Transportable en plataformas.

En cuanto a la reacción, el sistema dispone en cuanto a medidas *Softkill*:

- Inhibición simultanea de GPS y GLONASS.

- Antena “omnidireccional” o “directiva asociada a un posicionador” para trabajar como sistema esclavo de radar.
- Control de potencia para ajustar la distancia de inhibición.
- El control de potencia y el uso de antena directiva para perturbación de radioenlaces hasta 6GHz, junto con la utilización de la detección radar, permite generar un cono de inhibición con la potencia necesaria para inhibir el GPS a una distancia determinada. Esto reduce de manera muy significativa las inhibiciones colaterales de GPS a otros usuarios.

El sistema tiene la posibilidad del uso de medidas *Hardkill*, mediante la utilización de un dron para interceptar el dron hostil. Este dron de contramedidas debería estar a cubierto y desplegarse bajo las órdenes del operador. El la figura 16 se muestra la captura de un dron hostil mediante una malla (medida *Hardkill*).

(Indra, 2022) (Indra, ARMS Sistema Multisensor, 2019)

Figura 17. Captura mediante malla de dron hostil. Fuente Indra

3.3.4. Sistema CERVUS de Gradiant

CERVUS, o lo que es lo mismo, Sistema de Control de Equipos Remotos y Vehículos no Tripulados de Vigilancia Electrónica, está integrado con el sistema Captive, que consiste en un dron cautivo que es utilizado en funciones de vigilancia y guerra electrónica. El modo de operar del sistema *CERVUS* es el habitual, detección, clasificación y neutralización de aeronaves no tripuladas (mediante fusión de sensores). Se trata de un sistema modular, escalable. Ofrece la posibilidad de funcionar de forma autónoma o mediante operador. Dispone de tres módulos:

- SmartEar: destinado a la detección, clasificación y seguimiento de UAS mediante el análisis de radiofrecuencia.
- SmartEye: proporciona la detección, clasificación (modelo del dron) y seguimiento de UAS utilizando sensores electrópticos y de infrarrojos EO/IR y analizadores de video.
- SmartJam: es el módulo de neutralización. Genera una interferencia inteligente de forma de onda adaptativa que abarca las frecuencias típicas de operación (GNSS, comando y control). (Gradiant, 2022)

El sistema se presenta en dos configuraciones:

1. El fusil anti-dron conectado al equipo de inhibición configurado para proporcionar protección a instalaciones fijas. La potencia de inhibición es de 50 W por canal (total 400 W)
2. La otra configuración es en modo portátil. En una mochila se lleva el fusil y el operador se integra en una patrulla a pie. Tiene las mismas capacidades que la configuración anterior, aunque en este caso la potencia es de 25 W por canal (total 200 W).

Figura 18. Configuración en modo portátil. Fuente: Revista Ejército de Tierra nº 962

En la figura 15 se observa al operador del sistema apuntando a la amenaza, en la configuración de modo portátil.

CERVUS se compone de los siguientes subsistemas:

- Plataforma vehicular.
- Subsistema DDD (detección de drones). Es un sistema de detección, clasificación, seguimiento y neutralización de UAS basado en un sistema de mando con sensores de RF, radiogoniómetros y cámara con procesado de vídeo.
- Subsistema de antenas. Proporciona localización del dron detectado en coordenadas globales (localización sobre GIS) y alerta temprana mediante la detección del dron a una distancia mínima de 500 metros. Radiogoniómetro.
- Subsistema de visión. Clasificación y seguimiento. Identificación de tamaño del dron. Basado en una cámara IP todoterreno Full HD, de alta calidad en entornos muy extremos.
- Subsistema de izado. Mediante mástil telescópico neumático.
- Subsistema de dron cautivo. Proporciona identificación y localización mediante el sistema de observación que posee el sistema. Aumenta el campo de visión de las unidades terrestres y contribuye en la toma de decisiones.
- Subsistema de inhibición. Mediante fusil. Alta directividad. Consigue la neutralización de todos los drones comerciales que utilicen las frecuencias 2,4 GHz, 5,8 GHz y posicionado GNSS en 1,2 GHz y 1,5 GHz. Accionando el disparador del fusil RF, se consigue neutralizar las comunicaciones que recibe el dron. Dependiendo de la configuración del fusil, podremos forzar el aterrizaje controlado del dron, hacer que regrese a su punto de despegue con la finalidad de rastrearlo, dejarlo en vuelo estático o bloquear la transmisión de imágenes.

(Rodríguez Olmedo, 2021)

3.3.5. Sistema Aeroscope de DJI

Se trata de una antena de instalación fija y junto a su software puede detectar e identificar UAS y la ubicación del operador.

Sus características destacadas son:

- Detectar e identifica drones.
- Detectar drones con un alcance máximo de 50 kilómetros.
- Obtiene toda la información y se muestra en un mapa en un ordenador (función GIS).
- La telemetría del dron es transmitida al receptor Aeroscope.
- Cobertura de 360 grados.
- Ganancias de 8 ó 16 dBi.

- Módulos de frecuencia 2.4 Gz y 5.8 Gz.
- Identifica rápidamente la comunicación del UAS.
- Obtiene la ubicación del operador del dron.
- Obtiene el número de serie del dron.
- Indica la dirección y ruta del UAS (radiogoniómetro).
- Toda la Información se obtiene en tiempo real.
- Protección IP65 contra agua y polvo.

(Hobbytuxtla, 2021)

3.3.6. Sistema Horus Captor de Thales

La solución de Thales en sistemas C-UAS es el *Horus Captor*. El sistema tiene capacidad de detección, clasificación, identificación, seguimiento y neutralización de micro y mini drones en diversos escenarios.

La integración de diferentes elementos de detección, tanto activos (radar) como pasivos (radiogoniómetro), conceden al *Horus Captor* la protección de gran variedad de amenazas posibles. Es modular y escalable. Desde UAS comerciales radios comandados, hasta aquéllos que no utilizan radiofrecuencia, con trayectorias preprogramadas y vuelos inerciales, entre otros.

El dispositivo dispone de función GIS (Sistema de Información Geográfica), que permite trabajar con información georreferenciada.

El sistema dispone también de radiogoniómetros (detectores de frecuencias) para la localización de drones. Mediante el radiogoniómetro se realiza en el estudio del espectro radioeléctrico de los alrededores y se determina si procede de un dron o de una estación de control.

Fases del proceso de identificación (mediante fusión de sensores):

- El radar o el radiogoniómetro detecta y clasifica un dron potencial y proporciona unas coordenadas o una dirección.
- La cámara, utilizando un campo de visión ancho, se orienta automáticamente a la traza o a la dirección recibida. El operador sigue automáticamente la evolución de la traza en pantalla.
- El operador estrecha el campo de visión hasta que el dron es identificable.

Respecto a la función de inhibición, puede realizarla a la frecuencia de video o radiocontrol, produciendo un el regreso a la posición de origen del dron o un aterrizaje en la posición en la que se encuentre en ese momento. También es capaz de inhibir las bandas GPS. Esta función es muy efectiva, pero se debe restringir, sobre todo en entornos urbanos, porque puede afectar a servicios esenciales.

El sistema ofrece dos configuraciones de uso:

- Portátil. Para protección temporal. El sistema se puede desplegar en la zona a proteger en menos de 20 minutos por dos personas. En la figura 17 se muestra radar y sistema optrónico de la configuración portátil del sistema.
- Instalación fija. Para instalaciones que requieren una protección permanente.

Figura 19. Equipo anti-dron portátil. Fuente: Thales

Componentes del sistema:

- Radiogoniómetro.
- Radar (Squire, radar Doppler) 3D.
- Sistema Optrónico (Gecko Optronics, con cámaras diurna y térmica).
- Inhibidor (DroneCannon), El operador toma la decisión de accionar la inhibición para el

dron seleccionado con alta directividad. Ésta tiene un alcance de 2 km y se las bandas de frecuencia que se puede seleccionar son: 433 y 915 MHz, 2.4 y 5.8 GHz, GNSS.

- SW Horus X para operación del Sistema. El operador puede crear zonas de alarma sobre el mapa, para así descartar zonas sin interés.

(Thales, 2020)

3.3.7. Sistema ADRIAN de electrónica Roma

El sistema propuesto por electrónica Roma, se denomina ADRIAN (Anti-Drone Interception Acquisition Neutralization) y está destinado a la neutralización de drones de pequeño tamaño, que vuelan a baja altura y velocidad (C-UAS LSS), en multitud de entornos, urbanos y aislados.

Dispone de sensores radar, EO/IR, acústicos, de detección de enlace y radiogoniómetros, que posibilitan, mediante la fusión de datos de los sensores, la detección y la identificación de su tamaño y modelo. Posee arquitectura modular y escalable. Es transportable mediante plataformas.

Características:

- Arquitectura de detección multiespectral y multidominio (comunicación, radar, EO/IR, acústica).
- Configuración modular/escalable.
- Configuración fija o móvil.
- Eliminación *Softkill* de UAS por contramedida contra el sistema de Radio Control *jamming* (5,8 GHz) y GNSS.
- Falsificación de GNSS (*Spoofing*) para forzar el aterrizaje de drones en un área segura.
- Detección de señales de muy baja potencia y salto de frecuencia.
- Análisis de amenazas en tiempo real (clasificación, identificación, geolocalización GIS).
- HMI fácil de usar, con retroalimentación inmediata sobre alarmas y características de amenazas.
- Interfaz externa al Centro Operativo Central.
- Fácil despliegue y posibilidad de integración en vehículos móviles.
- Apoyo logístico para el mantenimiento y la reparación durante toda la vida.

(GROUP, 2020)

3.3.8. Sistema Drone Guard de Elta Systems

- **Funcionalidades**
  - Detección: acústico, sensor electro-óptico e infrarrojo, radar 3D, inteligencia de comunicaciones.
  - Clasificación: sensor electro-óptico e infrarrojo, Inteligencia de comunicaciones y radar.
  - Soluciones anti-dron: *Hardkill* y *Softkill*.

- **Plataformas**

Los sensores modulares pueden ser configurados para ser portátiles, en sitios fijos o en movimiento, configuraciones hasta 60 mph (es decir, en vehículos o en barco)

- **Drone guards sensores y sistemas**

Drone Guard es modular y escalable. Gracias a la fusión de sensores, el rendimiento óptimo de sistema se consigue cuando todos los sensores funcionan a la vez. No obstante, el sistema permite que los sensores puedan funcionar de forma independiente.

Además, el sistema posee arquitectura abierta, lo que permite que los sensores de otros

fabricantes se puedan incluir en la configuración de *Drone Guard*.

A continuación, se muestran los principales sensores de contramedidas que se pueden integrar en el Sistema *Drone Guard*.

- Radar (Rangos de hasta 14 Km). En la figura 20 se muestra radar de defensa aérea, 5ª generación de radares tácticos 3D. ELM-2026B/D

Figura 20. ELM-2026BF. Fuente: Elta Systems

- Detección RF, mediante radiogoniómetros, con interceptores *Softkill*, de acción directiva. Inhibición de señal GNSS. En la figura 21 se muestra dispositivo de detección RF con cobertura de frecuencia desde 400 MHz a 6 GHz, 360º y alcance por encima de 10 km.

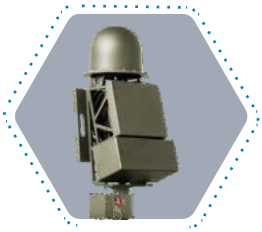

Figura 21. Detector RF. Fuente: Elta Systems

- EO/IR 360º de cobertura, identificación por encima de los 8 Km y detección por encima de los 15 Km. Clasifica la amenaza, identificando el tamaño y modelo del dron. En la figura 22 se muestra e sistema táctico *POPStar* "Sistema automático de detección de objetivos" de 360 grados, de aplicación en protección de aeropuertos, protección de instalaciones sensibles y control de fronteras.

Figura 22. POPStar. Fuente: Elta Systems

- Sistemas *HarKill* / *Softkill*
  - *ELK*-7009 Comunicación y GNSS de banda ancha bloqueador, figura 23.
  - *ELK-7009A* Toma el control y aterriza con seguridad los drones, tomando el RC (control remoto), figura 24.
  - *SMARTSIGHT* eliminación de cinética (disparo tenso), figura 25.
  - *Drone Kill Drone*. Impacto cinético mediante dron cazador, figura 26.
  - *ROCKNET* Cohete eléctrico autónomo para la interceptación de drones, figura 27.

Figura 23. ELK-7009. Fuente Elta Systems

Figura 24. ELK-7009A. Fuente: Elta Systems

Figura 25. Smartsight. Fuente: Elta Systems

Figura 26. Drone Kill Drone. Fuente: Elta Systems

Figura 27. Rocknet. Fuente: Elta Systems

(ELTA System, 2019)

3.3.9. Sistema Leonidas de Epirus

El sistema anti-dron *Leonidas* lo ha desarrollado la empresa californiana Epirus. Mediante este sistema se derribarían enjambres de drones instantáneamente mediante microondas de alta potencia. La producción de microondas se consigue mediante transistores de nitruro de galio, en lugar de los tubos de vacío del tradicional magnetrón, usados en radares durante décadas. En la figura 28 se muestra una simulación de derribo de un enjambre de drones.

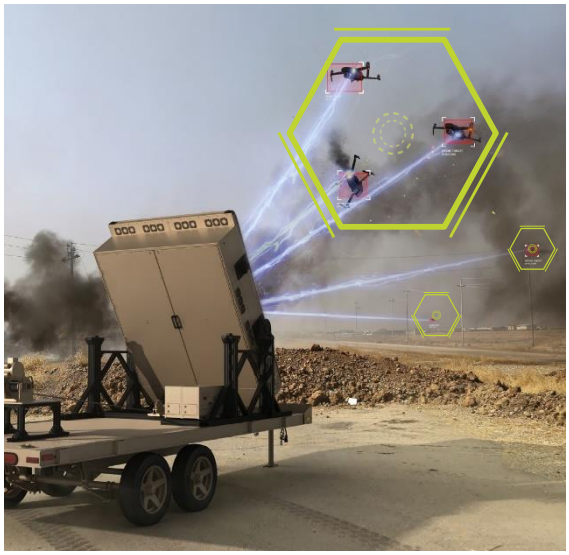

Figura 28. Simulación de funcionamiento Sistema Leonidas. Fuente: Epirus

El tamaño es portátil. Otra gran ventaja, que presenta el sistema frente a otros, es el manejo por software para desactivar objetivos electrónicos, mediante inhibición de señal GPS, de radioenlace hasta 6 GHz con mucha precisión (excelente directividad). De esta forma se ofrece a los operadores un control y seguridad excelentes, mediante fusión de sensores. La formación digital de haces permite una precisión milimétrica para que los operadores neutralicen las amenazas. En todos los sistemas Leonidas se

reducen drásticamente el tamaño, el peso y el consumo.

Funciona de manera muy eficiente a bajas temperaturas, lo que elimina la necesidad de soluciones de refrigeración. El sistema permite su uso a los pocos minutos de encenderlo. *Leonidas* tiene una arquitectura de sistema abierto y un diseño de hardware modular que emplea módulos amplificadores reemplazables en línea (LRAM), permitiendo su reparación en la zona de operación en menos de ocho minutos. Los LRAM actualizados se pueden implementar de inmediato en las unidades Leónidas para mejorar instantáneamente el alcance.

– **Características de Leonidas**

- Swarm Defeat: Permite la orientación simultánea y la neutralización de múltiples UAS.
- Precisión: la dirección de haz optimiza la potencia en el objetivo.
- Zonas de exclusión aéreas mediante localización GIS. Las zonas de exclusión aérea programables permiten que los UAS amigables viajen libremente mientras neutralizan los UAS hostiles.
- Interoperabilidad: La arquitectura de sistema abierto permite la integración con los sistemas de mando y control existentes de los usuarios para la detección, orientación y seguimiento de UAS.
- Transportable sobre plataformas móviles. Modular y escalable.
- Entorno operativo seguro: los bajos voltajes de funcionamiento evitan emisiones nocivas no deseadas para los operadores del sistema.
- Innovación en el núcleo: Epirus inventó *SmartPower*, que utiliza semiconductores de nitruro de galio (GaN) habilitados para producir niveles altos de potencia durante la transmisión.
- Múltiples casos de uso: ideal para una variedad de conjuntos de misiones, incluidos el enjambre de contra-UAS.

Figura 29. Sitema Leonidas montado sobre remolque. Fuente: Epirus

(Riccio, Di gianluca, 2021) (Epirus, 2022)

En la tabla 1 se indican, a modo de resumen, las características de los distintos sistemas, que según el Sr. Vázquez, Director de Desarrollo de Productos de Defensa y Vigilancia Electrónica de Indra, señaló como determinantes a la hora de la elección de un sistema C-UAS, anexo 1.

		Tabla 1																								
		AUDS	Blighter	Reino Unido	Dronedefender	Battelle	USA	ARMS	Indra	España	CERVUS	Gradiant	España	Aeroscope	DJI	China	Horus Captor	Thales	Francia	ADRIAN	Elettronica Roma	Italia	Drone Guard	Elta	Israel	Leonidas	Epirus	USA
Sensores	Radar	SI			NO			SI			NO			NO			SI			SI			SI			NO		
	EO/IR	SI			NO			SI			SI			NO			SI			SI			SI			NO		
	Radiogoniómetro 1D	NO			NO			SI			SI			SI			SI			SI			SI			NO		
	Radar 3D	NO			NO			SI			NO			NO			SI			NO			SI			NO		
	Acústico	NO			NO			SI			NO			NO			NO			SI			SI			NO		
	Radiogoniómetro 2D	NO			NO			NO			NO			NO			NO			NO			NO			NO		
Mando y control	Identificación tamaño dron	SI			NO			SI			SI			SI			SI			SI			SI			NO		
	Fusión de sensores	SI			NO			SI			SI			SI			SI			SI			SI			SI		
	Identificación modelo dron	SI			NO			SI			SI			NO			SI			SI			SI			NO		
	Localización sobre GIS	NO			NO			SI			SI			SI			SI			SI			NO			SI		
	Modular/Escalable	SI			NO			SI			SI			NO			SI			SI			SI			SI		
	Integración plataformas móviles	SI			NO			SI			SI			NO			NO			SI			SI			SI		
Sofkill	Perturbador de GPS	SI			SI			SI			SI			NO			SI			SI			SI			SI		
	Perturbación radioenlaces hasta 6 GHz	SI			SI			SI			SI			NO			SI			SI			SI			SI		
	Perturbación radioenlaces hasta 3 GHz	SI			SI			SI			SI			NO			SI			SI			SI			SI		
	Perturbación alta directividad	SI			SI			SI			SI			NO			SI			NO			SI			SI		
	Spoofing	NO			NO			NO			NO			NO			NO			SI			NO			NO		
Hardkill	Energía dirigida de microondas	NO			NO			NO			NO			NO			NO			NO			NO			SI		
	Laser de potencia	NO			NO			NO			NO			NO			NO			NO			NO			NO		
	Cohete teledirigido	NO			NO			NO			NO			NO			NO			NO			SI			NO		
	Disparo tenso	NO			NO			NO			NO			NO			NO			NO			SI			NO		
	Dron cazador	NO			NO			SI			NO			NO			NO			NO			SI			SI		
	Captura con malla	NO			NO			SI			NO			NO			NO			NO			NO			NO		

4. Análisis DAFO

Se realizará a continuación un análisis DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades), mediante el que se valorará si resulta adecuado dotar de sistemas anti-dron a instalaciones militares fijas, para su protección, tanto en zonas urbanas como aisladas.

Figura 30. Matriz DAFO. Fuente: elaboración propia

En la figura 30 se muestra la matriz DAFO, elaborada en base a los conocimientos adquiridos durante el desarrollo del presente TFG. Se comprueba que el cuadrante con más peso de la matriz es el de fortalezas, con siete ítems, seguido del cuadrante de oportunidades con seis ítems. Las debilidades y amenazas, tan sólo presentan tres y dos ítems en sus respectivos cuadrantes. Se puede concluir, en base a este análisis, que la adquisición de sistemas anti-dron para la protección de instalaciones militares fijas, quedaría razonadamente argumentada.

No obstante lo anterior, en la adquisición del sistema se tendrían que tener en cuenta las debilidades y amenazas puestas de relieve. El carácter tan sofisticado de estos sistemas requiere de un riguroso mantenimiento, además de una formación específica y profunda de sus operadores. No se debe eludir el riesgo fundado de producir daños colaterales por una mala praxis en su empleo, sobre todo en zonas urbanas. En atención a las amenazas detectadas, se deberá elegir un sistema flexible, de un fabricante con capacidad de reacción rápida en la implantación de nuevas funcionalidades ante la continua evolución de los UAS.

5. Análisis multicriterio

Para este análisis no se considerarán los siguientes sistemas:

- Anti-dron portátil *DroneDefender* de la empresa americana Battelle. Al tratarse de un sistema portátil, se empleará generalmente para protección temporal de objetivos móviles. No sería, por tanto, adecuado para la protección del escenario elegido como objetivo (instalaciones militares).
- Sistema *Aeroscope* de DJI. Se trata de una antena de detección de sistemas UAS, no pudiéndose considerar como sistema anti-dron.

5.1. Identificación y selección de los criterios

Los criterios seleccionados para la evaluación de los sistemas C-UAS ya fueron relacionados en la tabla 1. Se citan de nuevo y se hace una breve reseña de los mismos.

- Sensores, de diferente naturaleza y frecuencia de funcionamiento. Se valora la disponibilidad o no de diferentes tipos detectores de drones, lo que permite mejorar la probabilidad de detección y bajar la probabilidad de falsa alerta.

Tabla 2	
Sensores	Radar
	EO/IR cámara visible e infrarrojo
	Radiogoniómetro 1D
	Radar 3D
	Radiogoniómetro 2D
	Acústico

- Funciones de mando y control, donde se valora la disponibilidad o no de diferentes capacidades

Tabla 3	
Mando y control	Identificación tamaño dron
	Fusión de sensores
	Identificación modelo dron
	Localización sobre mapa GIS
	Modular/Escalable
	Integración plataformas móviles

- Contramedidas tipo *Softkill*, donde se valora la disponibilidad o no de diferentes tipos de perturbación y engaño.

Tabla 4	
Sofkill	Perturbador de GPS
	Perturbación radioenlaces hasta 5,8 GHz
	Perturbación radioenlaces hasta 3 GHz
	Perturbación alta directividad
	Spoofing

- Contramedidas tipo *Hardkill*, donde se valora la disponibilidad o no de diferentes tipos de capturadores y destructores de los drones.

Tabla 5	
Hardkill	Energía dirigida de microondas
	Láser de potencia
	Cohete teledirigido
	Disparo tenso
	Dron cazador
	Captura con malla

5.2. Selección del método de análisis multicriterio

El método será de tipo cuantitativo, de forma que, una vez seleccionados los parámetros de comparación, se tabularán y se asignará un valor numérico al cumplimiento o no por cada sistema. Al final se realizará la suma algebraica de los diferentes criterios de comparación para cada sistema, siendo el mejor el que obtenga la suma de mayor valor.

5.3. Determinación del peso relativo de cada criterio

Si un sistema posee la capacidad, se asignará el valor del 1 al 5 en función de la importancia del parámetro para el sistema, mientras que si no posee la capacidad se le asignará el valor "0".

En la tabla siguiente se indica el peso asignado a cada parámetro, en función del orden de importancia, establecido por el experto de Indra Sr. Vázquez (anexo 1), de los elementos necesarios para el sistema. No se considera el detalle de las características de la capacidad de cada elemento, por ser una información no pública en la mayoría de sistemas.

	Tabla 6	
	Criterio	**Peso**
Sensores	**Radar**	5
	EO/IR cámara visible e infrarrojo	4
	Radiogoniómetro 1D	3
	Radar 3D	2
	Radiogoniómetro 2D	2
	Acústico	1
Mando y control	**Identificación tamaño dron**	5
	Fusión de sensores	4
	Identificación modelo dron	3
	Localización sobre mapa GIS	3
	Modular/Escalable	2
	Integración plataformas móviles	1
Sofkill	**Perturbador de GPS**	5
	Perturbación radioenlaces hasta 5,8 GHz	4
	Perturbación radioenlaces hasta 3 GHz	3
	Perturbación alta directividad	2
	Spoofing	1
Hardkill	**Energía dirigida de microondas**	5
	Laser de potencia	4
	Cohete teledirigido	3
	Disparo tenso	2
	Dron cazador	2
	Captura con malla	1
	Total Puntuación	**66**

5.4. Realización de la ponderación de criterios

Tabla 7								
Peso Criterio SI=1-5, NO=0	Sistema	AUDS	ARMS	CERVUS	Horus Captor	ADRIAN	Drone Guard	Leonidas
	Fabricante	Blighter	Indra	Gradiant	Thales	Elettronica Roma	Elta	Epirus
	Pais	Reino Unido	España	España	Francia	Italia	Israel	USA
Sensores	Radar	5	5	0	5	5	5	0
	EO/IR	4	4	4	4	4	4	0
	Radiogoniómetro 1D	0	3	3	3	3	3	0
	Radar 3D	0	2	0	2	0	2	0
	Acústico	0	1	0	0	1	1	0
	Radiogoniómetro 2D	0	0	0	0	0	0	0
Mando y control	Identificación tamaño drone	5	5	5	5	5	5	0
	Fusión de sensores	4	4	4	4	4	4	4
	Identificación modelo drone	3	3	3	3	3	3	0
	Localización sobre GIS	0	3	3	3	3	0	3
	Modular/Escalable	2	2	2	2	2	2	2
	Integración plataformas móviles	1	1	1	0	1	1	1
Sofkill	Perturbador de GPS	5	5	5	5	5	5	5
	Perturbación radioenlaces hasta 6 GHz	4	4	4	4	4	4	4
	Perturbación radioenlaces hasta 3 GHz	3	3	3	3	3	3	3
	Perturbación alta directividad	2	2	2	2	0	2	2
	Spoofing	0	0	0	0	1	0	0
Hardkill	Energía dirigida de microondas	0	0	0	0	0	0	5
	Laser de potencia	0	0	0	0	0	0	0
	Cohete teledirigido	0	0	0	0	0	3	0
	Disparo tenso	0	0	0	0	0	2	0
	Dron cazador	0	2	0	0	0	2	2
	Captura con malla	0	1	0	0	0	0	0
Total Puntuación		38	50	39	45	44	51	31

Se puede observar en la tabla 2 que ningún dispositivo dispone de radiogoniómetro 2D, ni de láser de potencia. No obstante, no se eliminan de la ponderación por considerar que sería un valor añadido para el sistema si alguno incluyera estos elementos en un análisis futuro. El láser de potencia, en particular, fue considerado por el experto de Indra (anexo 1), en segundo lugar en importancia, en cuanto a medidas *HardKill* en la definición de .la configuración de un buen sistema C-UAS.

5.5. Identificación e implementación de la solución seleccionada

El sistema que alcanza la mayor puntuación es el *Drone Guard* de Elta. Se debe sobre todo a que posee sistemas de contramedidas de tipo *Hardkill*, para zonas aisladas/ zona de operaciones, no implementadas en el resto de sistemas analizados, excepto en el sistema *Arms* de Indra y Sistema *Leonidas* de Epirus. Este tipo de medidas, sobre todo la interceptación mediante cohete eléctrico y eliminación cinética mediante disparo, están totalmente desaconsejadas en zonas urbanas, debido al riesgo real de daños colaterales. No obstante, el *Drone Guard*, atendiendo a la variedad de medidas *Softkill* que implementa, estaría indicado también para su despliegue en zonas urbanas.

El siguiente sistema, en orden de puntuación, es el *ARMS* de Indra. Destaca sobre todo en la variedad de sensores que despliega y en particular en sus capacidades de mando y control, donde obtiene la máxima puntuación junto con el sistema *CERVUS* de Gradiant. El *ARMS* dispone además, de todas las medidas *Softkill* consideradas en el presente análisis excepto *Spoofing*. En cuanto a medidas *Hardkill*, dispone de dron cazador y captura con malla. Muy aconsejable, por tanto, para su despliegue tanto en zonas urbanas como aisladas/ zona de operaciones.

El *ARMS*, el *AUDS* de Blighter y el *CERVUS*, constituyen los C-UAS con los que cuentan las FAS actualmente. El *ARMS* obtiene bastante mejor valoración que *AUDS* y *CERVUS*.

Horus Captor de Thales logra la tercera posición con una buena puntuación. Destaca su radar 3D que sólo lo implementa el *ARMS* y el *Drone Guard*. Aunque este elemento sólo tiene como valor ponderado “2”, este tipo de radar permite medir el ángulo de llegada en elevación, además del acimut y la distancia.

El que peor valoración obtiene es el *Leonidas* de Epirus. Esto se debe a que no dispone de sensores de vigilancia y detección. Necesitaría operar integrado con un sistema de vigilancia y detección de otro fabricante. Destaca, sin embargo, en la utilización de microondas de alta potencia para el derribo de enjambres de drones, siendo el único C-UAS del estudio que dispone de esta medida *Hardkill*. Dispone además de una gran variedad de contramedidas *Softkill*.

Para concluir, los sistemas más completos son el *ARMS* y el *Drone Guard*. Ambos se podrían desplegar en instalaciones fijas (bases militares) tanto en zonas urbanas como en aisladas. Al tratarse el sistema *ARMS* de un sistema de fabricación nacional, sería éste el recomendado para su adquisición por las FAS.

6. Conclusión

Los sistemas UAS LSS suponen un riesgo creciente para cualquier sistema de defensa aérea. La proliferación de éstos se explica por el aumento de tecnologías, en gran parte de entretenimiento, aplicables a estos dispositivos. El bajo coste, la cantidad de ofertas en el mercado, facilidad de adquisición y simplicidad de manejo, hacen que este tipo de dispositivo esté al alcance de cualquier persona y para cualquier uso, incluido el malicioso.

La irrupción de los UAS LSS, dispositivos en su mayoría de pesos inferiores de 20 kg (categorías micro y mini según OTAN) ha puesto en compromiso la defensa aérea tradicional. La posibilidad de ser objeto de un ataque UAS LSS es, desgraciadamente, una realidad, según la opinión de expertos en la materia. La solución a esta nueva amenaza no implica la sustitución del actual concepto de defensa aérea, sino de complementarlo con sistemas anti-dron, C-UAS, que palíen estas limitaciones identificadas.

El objetivo que deben acometer los sistemas C-UAS es la detección y neutralización de la amenaza. Para la definición de la configuración de un sistema anti-dron es necesario el análisis del concepto de la operación. En este contexto es necesario el estudio de las fases de funcionamiento de vigilancia y conciencia situacional, mando y control y ayuda a la decisión y por último, la fase de reacción.

Para el establecimiento del modo operativo de los sistemas, es determinante el entorno a proteger de la amenaza. Fundamentalmente se distinguirán zonas urbanas y zonas aisladas (incluida zona de operaciones). Para los elementos de detección, ambas zonas pueden disponer de elementos similares (radares, sensores acústicos, sensores EO/IR, detectores de comunicaciones RF/radiogoniómetros y GPS), no obstante, en zonas aisladas las posibilidades de detección a gran distancia son más probables. En cuanto a las medidas de neutralización, en zonas urbanas, se utilizarán preferentemente medidas *Softkill* con sistemas de puntería, para conseguir directividad y de esta forma no interferir sistemas civiles. En zonas aisladas, las medidas pueden ser más contundentes, con medidas *Softkill* omnidireccionales en incluso medidas *Hardkill*.

Mediante un análisis DAFO, se ha podido justificar de manera concluyente lo apropiado de dotar a las Fuerzas Armadas de sistemas C-UAS para protección de instalaciones fijas. De los resultados obtenidos del análisis multicriterio, los sistemas más adecuados al objetivo del estudio, han sido el sistema *Drone Guard* de Elta y el *ARMS* de Indra, si bien, por tratarse Indra de una empresa nacional, ha sido el sistema *ARMS* el recomendado. Además, con este fabricante está garantizada la evolución del sistema, al tratarse de una empresa multinacional con amplia experiencia en el sector de Defensa. La dotación de sistema *ARMS* evolucionados sería una buena opción para la futura Fuerza 35.

Para finalizar, incidir en el hecho de que la rápida evolución de la tecnología, impulsa la aparición de nuevos UAS, cada vez más sofisticados, que pueden provocar la obsolescencia prematura de los sistemas C-UAS, tal y como se establecía en el análisis DAFO como amenaza. La evolución de los sistemas C-UAS será, por tanto, un reto permanente en el campo de la defensa, en las próximas décadas.

PÁGINA INTENCIONADAMENTE EN BLANCO

Bibliografía

1. AESA. (2019). *Aerocamaras Especialistas en Drones*. Obtenido de https://dronehibrido.com/es/
2. Aguilera, R. P. (2019). *El uso del dron y la vulneración al derecho a la privaciad*. Obtenido de https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/16859/AGUILERA%20RITA%20PAOLA.pdf?sequence=1
3. Aircraft Systems, C.-U. (Septiembre de 2019). *Homeland Security.* Obtenido de https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf
4. Battelle. (2021). *Battelle*. Obtenido de https://www.battelle.org/
5. BBC. (22 de enero de 2015). Obtenido de https://www.bbc.com/mundo/noticias/2015/01/150122_mexico_narcotrafico_ingenio_droga_an
6. BBC. (18 de abril de 2016). Obtenido de https://www.bbc.com/mundo/noticias/2016/04/160418_drone_choca_avion_heathrow_egn
7. BBC. (16 de mayo de 2016). *BBC*. Obtenido de https://www-bbc-com.translate.goog/news/av/uk-36302136?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc
8. Bhargav Patel, M. E. (1 de septiembre de 2019). *Counter-Unmanned Aircraft Systems Technology Guide.* Obtenido de Counter-Unmanned Aircraft Systems Technology Guide: https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf
9. Blázquez García, R. (2018). *Horizontes Defensa y Seguridad*. Obtenido de https://www.horizontesdefensayseguridad.net/wp-content/uploads/sites/3/2018/11/DESEI_LTER_PassiveRadar.pdf
10. Blighter. (2020). *Blighter Surveillance Systems*. Obtenido de https://www.blighter.com/
11. BOE. (29 de Diciembre de 2017). *Boletín Oficial del Estado*. Obtenido de https://www.boe.es/boe/dias/2017/12/29/pdfs/BOE-A-2017-15721.pdf
12. Defensa Gob, Estado Mayor de la Defensa. (2019). Obtenido de https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/01_CONCEPTO_NACIONAL_C-UAS_LSS_xPARA_WEBx.pdf
13. DEGAM, D. G. (01 de 12 de 2016). *Subdirección General de Publicaciones y Patrimonio Cultural.* Obtenido de https://publicaciones.defensa.gob.es/monografias-del-sopt-n-15-proyecto-rapaz-y-tecnologias-anti-rpas.html
14. El País. (13 de julio de 2021). Obtenido de https://elpais.com/espana/2021-07-13/la-policia-confisca-en-malaga-el-mayor-dron-dedicado-al-transporte-de-droga.html
15. ELTA System. (2019). *IAI.* Obtenido de https://www.iai.co.il/p/eli-4030-drone-guard
16. Epirus. (2022). Obtenido de https://www.epirusinc.com/products
17. Gavilán Jiménez, F. R. (noviembre de 2012). *Escuela Superior de Ingenieros de la Universidad de Sevilla*. Obtenido de http://aero.us.es/rvazquez/FGJ_thesis.pdf
18. Global Estrategy. (julio de 2020). Obtenido de https://global-strategy.org/la-evolucion-de-la-amenaza-uav-en-atentados-terroristas/
19. Gradiant. (2022). *Gradiant*. Obtenido de https://www.gradiant.org/
20. GROUP, E. (1 de enero de 2020). *Antidrones Elettronica Roma.* Obtenido de Antidrones Elettronica Roma: https://www.elt-roma.com/product/adrian
21. Guillén, C. (18 de Noviembre de 2019). *Securitecnia.* Obtenido de https://www.seguritecnia.es/tecnologias-y-servicios/drones/drones-hostiles-y-amenazas-emergentes-

2_20191118.html

22. Hobbytuxtla. (2021). *Hobbytuxtla*. Obtenido de https://www.hobbytuxtla.com/sistemas-antidrones/dji-aeroscope/
23. Indra. (25-27 de junio de 2019). *ARMS Sistema Multisensor*. Obtenido de https://www.icao.int/NACC/Documents/Meetings/2019/NACCDCA9/NACCDCA9P08sp.pdf
24. Indra. (1 de enero de 2021). *Indracompany*. Obtenido de Indracompany: https://counteruas.indracompany.com/
25. Indra. (2022). Obtenido de https://www.indracompany.com
26. Industry, D. (2022). *directindustry*. Obtenido de https://www.directindustry.es/prod/onyxstar/product-182275-1799796.html
27. Isdefe, C. (1 de Mayo-junio de 2016-2017). *horizontesdefensayseguridad*. Obtenido de horizontesdefensayseguridad: https://www.horizontesdefensayseguridad.net/wp-content/uploads/sites/3/2017/12/estadodelarte_sensores_jun2017_v1.pdf
28. Levy, J. (2021). *CNN en español*. Obtenido de https://cnnespanol.cnn.com/video/israel-iran-barco-mar-arabigo-estados-unidos-gran-bretana-jose-levy-cafe/
29. *Onyxstar* . (2022). Obtenido de https://www.onyxstar.net/hydra-12/
30. Riccio, Di gianluca. (15 de abril de 2021). *Futuro prossimo*. Obtenido de Futuro prossimo: https://es.futuroprossimo.it/2021/04/leonidas-arma-mobile-a-microonde-che-distrugge-interi-sciami-di-droni/
31. Rodríguez Olmedo, J. I. (2021). Proyecto CERVUS. *REVISTA DEL EJÉRCITO DE TIERRA ESPAÑOL Nº 962*, 94 -101.
32. Thales. (2019). *Dossier Sistemas antidrone.*
33. Thales. (29 de octubre de 2020). *Thalesgroup*. Obtenido de Thalesgroup: https://www.thalesgroup.com/sites/default/files/database/document/2019-06/version-web_AF%20eDossier%206%20Sistemas%20Antidrones%204.pdf
34. *Zona Militar*. (14 de mayo de 2021). Obtenido de https://www.zona-militar.com/2021/05/14/la-fuerza-aerea-israeli-derriba-un-dron-de-hamas/

Anexos

Anexo 1: Entrevista a experto de Indra D. Francisco Vázquez Vázquez (Director de Desarrollo de Productos de Defensa y Vigilancia Electrónica de Indra)

Entrevista:

Desgraciadamente determinados grupos (terroristas, narcotraficantes, etc.) han visto en los drones una óptima oportunidad de mejorar sus actividades delictivas. Es necesario que las autoridades públicas refuercen todas las medidas a su alcance para evitar que el uso de los drones se convierta en un serio peligro para la sociedad y adoptar una serie de medidas subjetivas (policía, operadores y pilotos) y objetivas. Por ello hay que dotar de más medios y entrenamiento a las Fuerzas y Cuerpos de Seguridad del Estado. Por tanto, ante la reciente y continua amenaza de los UAS en fronteras, tráfico de drogas, contrabando, etc.

1. **¿Es consciente su empresa de hasta qué punto supone una amenaza el uso UAS con objetivos delictivos?**

   - Indra es consciente de la amenaza, y desde su Unidad de "Defensa y Seguridad" desarrolla diferentes soluciones de detección y neutralización de drones. Grupos terroristas, con unos mínimos recursos económicos, pueden disponer de dispositivos capaces de portar diferentes tipos de armas y poner en compromiso cualquier procedimiento de defensa aérea. Tanto la altura de vuelo como su velocidad, en drones de pequeño tamaño, es similar a la de cualquier pájaro, como puede ser el caso de las aves rapaces y esto dificulta enormemente su detección, al reflejar firmas radar muy pequeñas, inferiores a 5 decibelios por metro cuadrado.

2. **¿Qué riesgos puede suponer el empleo de drones?**

   - Las capacidades de un dron para realizar actividades que puedan suponer riesgos son innumerables. Estos dispositivos son capaces de llegar con facilidad a un determinado objetivo, desde famosos empresarios, políticos o líderes mundiales, hasta determinados puntos sensibles, como centrales nucleares, aeropuertos, edificios de gobierno, etc. Pueden atentar sin apenas riesgos para el ejecutante. Pueden volar portando explosivos y hacerlos detonar contra el objetivo seleccionado. No es descartable la posibilidad de emplear estos dispositivos como portadores de armas de destrucción masiva: armas químicas, biológicas o incluso nucleares.

3. **¿Dispone su empresa de algún sistema anti dron que ayude a vigilar o detectar para neutralizar esta amenaza?**

   - La solución de INDRA para la detección y neutralización de drones es el sistema *ARMS*.

4. **¿Podría describir sus características principales?**

   - Este sistema es capaz de detectar, rastrear, identificar y neutralizar sistemas aéreos no tripulados. Utiliza radares de alta resolución para detectar amenazas de pequeño y gran tamaño a kilómetros. Mediante cámaras de visión nocturna y diurna identifica de forma automática los drones y determina si suponen una amenaza. En este caso el sistema recoge toda la información posible, identificando el tipo de dron, cómo se comunica, cómo recibe la información e incluso dónde está el piloto. Si se confirma la amenaza y el dron invade la zona protegida, el sistema lo neutraliza. Para ello emplea un sistema de interferencias que interrumpe el guiado de la aeronave.

5. ¿Cree que el sistema *ARMS* podría satisfacer las necesidades de nuestras Fuerzas Armadas en la lucha contra los sistemas UAS?

- El sistema ARMS es flexible y capaz de adaptarse a las necesidades de los usuarios incorporando los componentes adecuados. Es idóneo para proteger tanto aeropuertos como bases militares o instalaciones singulares. También tiene la posibilidad de proteger superficies más amplias mediante el trabajo conjunto de varios sistemas *ARMS*. El sistema fue adquirido por el Ministerio de Defensa y actualmente se encuentra desplegado en Mali.

6. Si Vd. Tuviera que asesorar a nuestras Fuerzas Armadas en la adquisición de un sistema anti dron ¿podría relacionar por orden de importancia las características o elementos necesarios?

En líneas generales el sistema constará de sensores, sistema de mando y control y las contramedidas que adopta ya sean *Softkill* o *Hardkill*.

- Para el caso de los sensores:

  - El más importante es el **radar**, dado que es el sensor que permite detectar un dron muy rápidamente (del orden de 1 segundo) para poder tener tiempo de reacción para su neutralización.
  - El segundo sensor en importancia es la **cámara infrarroja y visible** que debe ser comandada por el radar para apuntar a la posible amenaza. Permite confirmar que se trata de un dron e identificar el tipo de dron (multirrotor, ala fija, etc). Este sensor sirve también para medir la elevación y el acimut del dron con precisión y por tanto poder apuntar las contramedidas directivas.
  - Le sigue en importancia el **radiogoniómetro**, sensor que permite detectar los radioenlaces/datalink tanto de control de vuelo como de transmisión de datos e imágenes de las cargas de pago de los drones. A pesar de ser un sensor de detección muy rápida (del orden de 1 segundo), no es tan seguro como el radar, porque el dron puede volar en silencio radio volando de forma autónoma (sin piloto que lo comande vía radioenlace).
  - **Radar 3D**, permite medir el ángulo de llegada en elevación, además del acimut y la distancia. Aunque es un parámetro importe, no es imprescindible para tener un buen sistema anti dron dado que lo puede medir la cámara IR y son radares más caros que los 2D.
  - **Radiogoniómetro 2D**, permite medir el ángulo de elevación, además del acimut. Aunque es un parámetro importe, no es imprescindible para tener un buen sistema anti dron dado que lo puede medir la cámara IR y son radiogoniómetros más caros que los 1D.
  - **Sensor acústico**, se le asigna el menor peso, ya que su alcance de detección es pequeño (tiempo de reacción pequeño).

- Para el sistema de Mando y Control:

  - **Identificación del tamaño** del dron, disponer de los algoritmos que determinen este parámetro es muy importante de cara evaluar la peligrosidad del dron y decidir el tipo de contramedida para su neutralización.
  - **Fusión de sensores**, disponer de esta capacidad es importante para bajar los falsos positivos y para mejorar los parámetros de medida de los drones, eligiendo el de mayor calidad de cada sensor.
  - **Identificación del modelo** de dron, permite elegir de forma más precisa la contramedida, pero es un parámetro difícil de medir y por tanto no muy fiable.
  - **Localización sobre mapa** (GIS). Permite hacer seguimiento por parte del operador de la trayectoria del dron, así como definir zonas de alerta sobre el mapa de forma que se genere una alarma cuando se traspasa la línea definida de la zona a proteger.

- **Modular/Escalable**. Que el sistema sea modular permite configurar el sistema de acuerdo a las necesidades con más o menos sensores y elementos de contramedidas, además de permitir su crecimiento añadiendo módulos con nuevas capacidades.
- **Integración plataformas móviles**. Permite operarlo como sistema táctico en movimiento para despliegues en zonas de operaciones.

- Contramedidas *Softkill*:

  - **Perturbador de GPS**. Es la contramedida más eficaz, al inhibir el sistema de navegación más importante del dron.
  - **Perturbador de radioenlace hasta 5,8 GHz**. Permite cortar la comunicación entre el dron y su operador, impidiendo su pilotaje por radiocontrol y la transmisión de datos desde el dron.
  - **Perturbador de radioenlace hasta 3 GHz** (peso 3). Permite cortar la comunicación entre el dron y su operador, impidiendo su pilotaje por radiocontrol y la transmisión de datos desde el dron. Tiene menor peso porque ya empiezan a aparecer sistemas de radioenlace en drones que trabajan a mayor frecuencia.
  - **Perturbación alta directividad**. Permite la perturbación con mucha selectividad espacial, ideal para aeropuertos donde es peligroso interferir a los sistemas de navegación y comunicación de los aviones.
  - ***Spoofing***. Permite suplantar a los satélites de forma que engaña a los GPS de los drones, indicándole una posición errónea. No se le da mucho peso porque son aún sistemas poco maduros y por tanto poco fiables.

- Contramedidas *Hardkill*:

  - **Energía dirigida de microondas**. Permite neutralizar los drones produciendo una alta interferencia en los sistemas electrónicos, que dejan de funcionar correctamente o destruirse.
  - **Energía dirigida por LASER de potencia**. Permite neutralizar los drones produciendo su destrucción física. El inconveniente frente a los de microondas, es que son sistemas más caros y que necesitan mucha energía para funcionar.
  - **Cohete teledirigido**. Permite destruir físicamente el dron. Son sistemas caros y que solo se puede usar en zonas despobladas
  - **Disparo tenso**. Permite destruir físicamente el dron. Son sistemas caros y difíciles de usar en zonas pobladas.
  - **Dron cazador**. El inconveniente frente a los sistemas anteriores es su tiempo de respuesta, al necesitar maniobras de despegue y tiempo de vuelo hasta el dron objetivo.
  - **Captura con malla**. Permite derribar al dron lanzándole una malla con una especie de fusil. El inconveniente es su poca distancia de uso y su baja fiabilidad.

7. ¿Conoce Vd. otros sistemas anti dron existentes el mercado que puedan competir con el sistema *ARMS* de INDRA?

- Actualmente como competidores del sistema *ARMS* podemos citar el *Horus Captor* de Grupo francés Thales, *ADRIAN* de la empresa italiana Electrónica Roma, el sistema estadounidense *Leonidas* de Epirus y *Drone Guard* israelí de Elta System.

Anexo 2: Entrevista a experto en UAS del Regimiento de Artillería Antiaérea 71

Entrevista al Tte. D. Alberto Bermejo Vesga, Jefe de Sección en la 11ª Batería 35/90 Skydor del Grupo de Artillería Antiaérea I/71.

Entrevista:

Desgraciadamente determinados grupos (terroristas, narcotraficantes, etc.) han visto en los drones una óptima oportunidad de mejorar sus actividades delictivas. Es necesario que las autoridades públicas refuercen todas las medidas a su alcance para evitar que el uso de los drones se convierta en un serio peligro para la sociedad y adoptar una serie de medidas subjetivas (policía, operadores y pilotos) y objetivas. Por ello hay que dotar de más medios y entrenamiento a las Fuerzas y Cuerpos de Seguridad del Estado. Por tanto, ante la reciente y continua amenaza de los UAS en fronteras, tráfico de drogas, contrabando, etc.

1. **¿Está al tanto de la amenaza que supone los UAS?**

   - Sí, en el Regimiento de Artillería Antiaérea 71 hemos sido durante un par de años Unidad de Referencia para la preparación ante este tipo de amenazas. Ello ha conllevado que hubiese grupos de trabajo, experimentos de diversos tipos y, en general, que todos tengamos un conocimiento más o menos importante acerca de la amenaza UAS (que es como oficialmente se denomina en el seno de las Fuerzas Armadas).

2. **¿Qué riesgos puede suponer el empleo de drones?**

   - Su bajo coste, su baja firma radárica y su amplia disponibilidad hacen del empleo de drones una gran amenaza ya que ni los sistemas ni los procedimientos de los que se disponían para la defensa aérea no tenían las capacidades para detectarlos ni neutralizarlos. Esto convierte a los UAS en una herramienta inquietante que pueden hacer uso de ella tanto grupos terroristas o insurgentes hasta ejércitos convencionales como hemos visto por ejemplo en el conflicto entre Armenia y Azerbayan.

3. **¿Hasta qué nivel es consciente de la amenaza de los drones (UAS)?**

   - Por el papel como Unidad de Referencia en el Regimiento, plenamente consciente.

4. **¿Conoce algún sistema que ayude a vigilar o detectar para neutralizar esta amenaza?**

   - Sí, varios. Trabajamos actualmente con el sistema *AUDS*, *Aeroscope* y *DroneDefender*.

5. **¿Cree que debería implantarse distintos tipos sistemas anti-drones debido a las incidencias últimas que ha habido con la amenaza de drones en Zona de Operaciones y/o Operaciones permanentes?**

   - Sí, se poseen registros actualizados de incidentes con drones en prácticamente en casi todas las zonas de operaciones. A raíz de ello ya varias de ellas se han instalado sistemas anti-drones.

6. **¿Conoce los diferentes tipos de UAS que posee en Zona de operaciones y/o operaciones permanentes?**

   - Diría que los reglamentarios del ejército, los que se usan para labores de inteligencia para pequeñas unidades.

7. **¿Y los diferentes tipos de sistemas que tienen para detectar drones?**

   - *AUDS* con su sistema radárico y *Aeroscope* con su sistema detector de la señal de comunicación entre

el UAS y el mando a distancia.

8. ¿Qué medios conoce de UAS? ¿Cuenta en su orgánica con alguno?

- Conozco los drones populares del mercado, los diversos DJI, que son con los que hemos trabajado en los experimentos de detección y neutralización llevados a cabo en la unidad. Orgánicamente no tenemos ninguno.

9. ¿Considera que se debería mejorar la tecnología para poder combatir contra esta amenaza?

- Sí, dado el gran éxito y crecimiento del mercado, las características de los drones están en constante mejora. Se necesita detectar más señales de control aparte de las de los drones de marca DJI, mayor capacidad de detección, mayor alcance…

10. ¿Cuenta con los medios suficientes para la mejora de la tecnología de drones?

- El éxito del mercado y su popularización hace que tanto las empresas privadas como los estados a través de la industria de defensa estén invirtiendo mucho en su mejora, por lo que seguro se puede esperar que haya una mejora constante de la tecnología.

11. ¿Tienen drones contramedidas (*Hardkill*) para interceptar drones hostiles?

- No, y no se está trabajando por lo que sé en tales drones, al menos no en su adquisición y su uso procedimental en el ejército.

Anexo 3: Entrevista a experto en UAS del Regimiento de Guerra Electrónica 31

Entrevista al Brigada D. Ricardo Rodríguez Baña, Integrante de la Sección de Estudios y Proyectos del CCAL del Regimiento de Guerra Electrónica 31.

Entrevista:

Desgraciadamente determinados grupos (terroristas, narcotraficantes, etc.) han visto en los drones una óptima oportunidad de mejorar sus actividades delictivas. Es necesario que las autoridades públicas refuercen todas las medidas a su alcance para evitar que el uso de los drones se convierta en un serio peligro para la sociedad y adoptar una serie de medidas subjetivas (policía, operadores y pilotos) y objetivas. Por ello hay que dotar de más medios y entrenamiento a las Fuerzas y Cuerpos de Seguridad del Estado. Por tanto, ante la reciente y continua amenaza de los UAS en fronteras, tráfico de drogas, contrabando, etc.

1. ¿Está al tanto de la amenaza que supone los UAS?

- Actualmente gran parte de la Sociedad, tiene conocimiento sobre la existencia de aeronaves no tripuladas, comúnmente conocidos como drones, y su uso lo asocian al ámbito lúdico o profesional, pero no se tienen en cuenta la amenaza que supone la inserción de cargas explosivas, sustancias estupefacientes o de contrabando, o simplemente la captación de imágenes no autorizadas o vuelos no autorizados con las consecuencias que conlleva ante alguna incidencia sobre la aeronave que pueda suponer un riesgo a una zona en cuestión. También hay que tener en cuenta la amenaza que supone de dotar a la aeronave de diversas cargas de pago, entre las que están dispositivos de captación de datos masivos, como parámetros técnicos de telefonía móvil, dar capacidad a la aeronave de dispositivos de inhibición de señales o de captación de señales diversas, lo que supone una violación de las leyes vigentes. Pero gracias a las numerosas fuentes de información de que se dispone actualmente, la Sociedad puede coger concienciación sobre las amenazas reales que supone la presencia de los UAV.

2. ¿Qué riesgos puede suponer el empleo de drones?

- Entre los posibles riesgos que se asumen en el empleo de UAS, se pueden tener en cuenta los siguientes, en el ámbito militar:
  - Ser detectado de manera visual o por la interceptación del canal de comunicaciones de radiofrecuencia o wifi
  - Ser neutralizado, perdiendo el control de la aeronave, lo que puede llegar a que se apropien de la aeronave o que la aeronave regrese al punto de origen y que pueda desvelar la posición del piloto, actuando directamente sobre el canal de comunicación o sobre la señal GPS mediante acciones de *jamming* o de *spoofing*
  - Ser derribado, por Sistema *Hardkill*, con consecuencias que van desde el riesgo de daños sobre el personal que se pueda estar sobrevolando o la interceptación de las posibles cargas de pago de que disponga la aeronave con el riesgo de pérdida de la seguridad de la información.

3. ¿Hasta qué nivel es consciente de la amenaza de los drones (UAS)?

- En el ámbito militar, el nivel de conocimiento de la amenaza de UAS se puede considerar alto, ya que en toda Unidad se es consciente de los riesgos que conlleva que se pueda realizar una acción táctica con el uso de UAS. aunque la mayoría del personal lo asocia a la captación de imágenes no autorizadas o la inserción de cargas explosivas a una zona de intereses. No obstante, en el ámbito de las unidades de EW, se tiene más conocimiento sobre la amenaza que supone el uso de EW, dependiendo de la carga de pago de que se disponga sobre la aeronave, no solo limitándola a cámaras de video o cargas explosivas.

4. ¿Conoce algún sistema que ayude a vigilar o detectar para neutralizar esta amenaza?

- En nuestro ámbito hay diversos sistemas que intercepten la amenaza de UAS y si se considera necesario neutralizarlos.

- Entre lo que podemos mencionar está el sistema *Arms* de Indra, con capacidades radar y de radiofrecuencia, así como el uso de perturbadores. También es de mencionar el Sistema *AUDS*, de dotación en el RAAA basado en el uso de un radar y la inhibición de radiofrecuencias. Luego está el sistema *Aeroscope* de DJI, que intercepta y extrae todos los datos de los UAS de la zona de cobertura de la marca DJI.
- Mención especial el sistema *CERVUS* del REW31, basado en un sistema totalmente pasivo de interceptación de radiofrecuencias y protocolos de comunicaciones UAS para la protección de la fuerza, en los que aparte dispone de un módulo de inteligencia de imágenes para el seguimiento visual de la aeronave, todo ello complementado con sistemas portátiles de inhibición de radiofrecuencias.

5. ¿Cree que debería implantarse distintos tipos sistemas anti-drones debido a las incidencias últimas que ha habido con la amenaza de drones en Zona de Operaciones y/o Operaciones permanentes?

- Efectivamente, se ve necesario que en todas las zonas de operaciones en las que esta desplegado las fuerzas españolas, se disponga de sistemas C-UAS, ya sea para su detección como la neutralización de dichas amenazas. Se puede tener en cuenta que se disponga de sistemas fijos en las diferentes bases, así como sistemas móviles que puedan dar apoyo a las unidades motorizadas o en bases de patrullas temporales, en este caso sistemas como el *CERVUS* encajan en esa versatilidad de empleo en cualquier circunstancia, gracias a su gran movilidad.

6. ¿Conoce los diferentes tipos de UAS que posee en Zona de operaciones y/o operaciones permanentes?

- En nuestro caso, se conocen las aeronaves oficiales que tienen en dotación ciertas Unidades, como suelen ser los RAVEN en los Batallones del CG de la Brigadas. Pero a nivel interno, puede que las Unidades hayan adquirido ciertos modelos comerciales para su uso para captación de imágenes, por ello la importancia de que cuando se despliega en alguna zona de operaciones se tenga acceso a todos los modelos de RPA que hay desplegados y confeccionar una lista blanca de aeronaves “amigas” para su control y conocimiento.

7. ¿Y los diferentes tipos de sistemas que tienen para detectar drones?

- Así es, en nuestro caso tenemos conocimiento de los diferentes sistemas de detección y neutralización que tienen las diferentes Unidades (*AUDS*, *Aeroscope*, *Arms*…) no solo por el conocimiento en si de la existencia de esos sistemas, sino también para identificar las deficiencias o mejoras para el sistema *CERVUS.*

8. ¿Qué medios conoce de UAS? ¿Cuenta en su orgánica con alguno?

- El UAS más conocido dentro del ámbito de las FFAA es el RAVEN, en el caso de ciertas Unidades se dispone de diferentes modelos comerciales. En este caso en particular se dispone de modelos DJI como el *Matrice* 300 o modelo como el *Phatom*, todo ellos de adquisición comercial.

9. ¿Considera que se debería mejorar la tecnología para poder combatir contra esta amenaza?

- Los medios de que se dispone se deberían de ir actualizando constantemente según van avanzado las tecnologías, por ello la importancia de ir evolucionando los sistemas ante nuevas amenazas (nuevas frecuencias, protocolos de comunicación, plataformas…), siendo de vital importancia la mejora de las diferentes tecnologías de que se dispone actualmente.

10. ¿Cuenta con los medios suficientes para la mejora de la tecnología de drones?

- Se podría confirmar que si se cuenta con los medios suficientes para ir mejorando las tecnologías, desde el punto de vista económico, hay un gran impulso por parte de las autoridades para dar soluciones ante este tipo de amenazas y el aprovechamiento del uso de UAS,s en beneficio propio. Es de gran

importancia contactos con las empresas y acudir a las diferentes ferias/exposiciones que se desarrollan relativas a UAS,s a lo largo del año, como SECUDRON, FEINDEF… donde se van distinguiendo cuales son las últimas tendencias en el ámbito de los UAS,S.

11. ¿Tienen drones contramedidas (*Hardkill*) para interceptar drones hostiles?

- No son muchos los casos en los que los propios UAS disponen de contramedidas para interceptor o neutralizar UAS hostiles, únicamente podría nombrar cierta capacidad de interceptación física por parte de UAS que consiste en disponer de un sistema de suelta de una red que “captura” el UAS hostil al soltar la red sobre él. Sería interesante de UAS con cierta carga de pago de perturbación, para neutralizar UAS hostiles, sin que esa perturbación afecte al UAS, disponiendo un enlace de comunicaciones ajeno a la banda de inhibición que se esté barriendo.

Anexo 4: Entrevista a experto en UAS del BCG de COMGEMEL

Entrevista a Brigada Integrante del Centro de Integración y Difusión de Inteligencia en COMGEMEL.

Entrevista:

Desgraciadamente determinados grupos (terroristas, narcotraficantes, etc.) han visto en los drones una óptima oportunidad de mejorar sus actividades delictivas. Es necesario que las autoridades públicas refuercen todas las medidas a su alcance para evitar que el uso de los drones se convierta en un serio peligro para la sociedad y adoptar una serie de medidas subjetivas (policía, operadores y pilotos) y objetivas. Por ello hay que dotar de más medios y entrenamiento a las Fuerzas y Cuerpos de Seguridad del Estado. Por tanto, ante la reciente y continua amenaza de los UAS en fronteras, tráfico de drogas, contrabando, etc.

1. **¿Está al tanto de la amenaza que supone los UAS?**

   - Sí, estoy al tanto de la amenaza, estamos muy centrados en este asunto.

2. **¿Qué riesgos puede suponer el empleo de drones?**

   - Los drones son el perfecto medio IMIL para suponer para nosotros una gran vulnerabilidad porque es un medio de obtención de información que utilizan medios ópticos, sensores, radar asociados a una cámara.

3. **¿Hasta qué nivel es consciente de la amenaza de los drones (UAS)?**

   - Entre nivel operacional, táctico y estratégico, hasta nivel estratégico. En el batallón de la BRIPAC tienen drones RAVEN que son de nivel táctico o incluso operacional, mientras otros tipos de drones como los Reaper son de nivel estratégico.

4. **¿Conoce algún sistema que ayude a vigilar o detectar para neutralizar esta amenaza?**

   - Conozco sistemas anti-drones, si se trata de un dron como puede ser un Predator puede ser detectado perfectamente por un radar. Dependiendo del tamaño del dron se emplearán un Sistema u otro. También, conozco el caza dron que perturba la señal entre el operador y el dron con el fin de que se pierda la comunicación entre ambos. En el caso de que se trate de un dron de gran tamaño se utilizará Defensa Antiaéreo.

5. **¿Cree que debería implantarse distintos tipos sistemas anti-drones debido a las incidencias últimas que ha habido con la amenaza de drones en Zona de Operaciones y/o Operaciones permanentes?**

   - Sí, debería implantarse. Cuento desde mi experiencia, cuando estuve de misión en Irak había una base americana, en la que había personal civil de mantenimiento y había algunos operadores que le gustaba manejar drones y sobrevoló la base en la que estábamos con un dron, con la incertidumbre en ese momento de no saber la procedencia del dron. Al no disponer de perturbadores no pudimos neutralizarlo.

6. **¿Qué impacto tendría y en qué nos afectaría una amenaza de drones en Zonas de Operaciones y/o Operaciones permanentes?**

   - Tiene un gran impacto, por ejemplo, los drones que son demasiados pequeños, los grupos terroristas los utilizan para tirar granadas contra las Fuerzas y Cuerpo de Seguridad del Estado. Supone una gran amenaza el tema de los drones porque se puede hacer una gran variedad de acciones, ya sea para bien o con ánimo de lucro.
   - Los drones pueden realizar acciones desde lanzar un explosive hasta hacer un reconocimiento de lugares sensibles para obtención de información.

7. **¿Conoce los diferentes tipos de UAS que posee en Zona de operaciones y/o operaciones permanentes?**

   - Sí, creo que lo que ahora están en Zona de Operaciones son los RAVEN y los drones “mosquitos”.

8. **¿Y los diferentes tipos de sistemas que tienen para detectar nuestros drones?**

   - Para drones de gran tamaño se usan los Radares y para drones pequeños se les puede detectar por la frecuencia que emite.

9. **¿Qué medios conoce de UAS? ¿Cuenta en su orgánica con alguno?**

   - Air Fun, Predator, Reaper, Neon, RAVEN etc. Cada Brigada tiene su propio dron, RAVEN. Lo concentran en la BRIPAC. Normalmente los Batallones disponen de RAVEN que tienen una autonomía de 10 kilómetros y la Brigada tiene un alcance los drones de hasta 20 Kilómetros y a nivel de ejército de hasta 100 kilómetros. En el ejército del Aire tienen drones mucho más grandes como los Predator. Tenemos Unidad de UAS pero no está creada por falta del personal y el material está en Almería.

10. **¿Le parece necesaria la adquisición de este tipo de medios a su nivel?**

    - Por supuesto, es lo más novedoso hoy en día, todo funciona con targeting para tener visión directa sobre el objetivo. Sobre todo, para evitar daños colaterales.

11. **¿Debería el ejército implantar alguna Unidad en la cual se emplee diferentes tipos de sistemas anti-drones? ¿Por qué? Si es sí, ¿Cuáles cree?**

    - Sí, debería ser las Unidades Antiaéreas porque son las más dotadas. Pienso que las Unidades Antiaérea debería ser las que tengan perturbadores para neutralizar drones, ya que disponen de los medios suficientes para poder realizarlo y se encargan del espacio aéreo. Además, las Unidades de Transmisiones podrían ser una posibilidad.

12. **¿Hay personal especializado, operadores de UAS y que tengan conocimientos sobre los tipos de sistemas anti-drones?**

    - Aquí en Melilla como ya he dicho no tenemos personal suficiente para crear una Unidad y por tanto aquí en el CIDI no tenemos ningún operador. Sin embargo, la Compañía de Transmisiones o de Artillería tienen algunos operadores y cada vez son más los que abundan en esta empresa.

13. **¿Cuánto coste tienen invertido o qué consideran invertir para la implementación de sistemas para la protección en Zonas de Operaciones contra los UAS?**

    - Desconozco realmente lo que se invierte en la implementación de los sistemas Anti-drones.

14. **¿Considera que se debería mejorar la tecnología para poder combatir contra esta amenaza?**

    - Claro, en un futuro creo que estos sistemas serán lo primordial pero no sólo para el combate sino también para velar por la seguridad de las personas.

15. **¿Cuenta con los medios suficientes para la mejora de la tecnología de drones?**

    - Aquí, no tenemos los medios suficientes, como ya he dicho, los materiales están en Almería donde hay una Unidad perteneciente a Melilla.

16. **¿Tienen drones contramedidas (*Hardkill*) para interceptar drones hostiles?**

- Tengo entendido que se trata de un dron que se encarga de interceptar el dron enemigo, pero no disponemos de este tipo de Sistema.

Anexo 5: Entrevista a experto en UAS del BCG de COMGEMEL

Entrevista a Subteniente integrante del Centro de Integración y Difusión de Inteligencia en COMGEMEL.

Entrevista:

1. **¿Está al tanto de la amenaza que supone los UAS?**

   - Sí estoy al tanto, aunque no siempre somos conscientes de ello, no sé hasta qué punto estamos preparados o acometemos la actitud necesaria para impedir la acción directa de los UAS sobre nosotros o a Unidades o incluso en la vida civil. Todo esto en función de las características de los drones.

2. **¿Qué riesgos puede suponer los drones?**

   - Podemos diferenciarlos en función de su función principal, seguimiento, vigilancia o ataque. Depende del entorno, normalmente son de vigilancia. En Zona de Operaciones y/o Operaciones permanentes no podemos evadirnos de la vigilancia de algún dron o algún UAS, nosotros tenemos asignado nuestra misión y debería haber Unidades que tengan asignado la detección de drones pero la realidad es que no hay.

3. **¿Hasta qué nivel es consciente de la amenaza de los drones (UAS)?**

   - Somos conscientes, pero no podemos actuar, tenemos que conocer la existencia de esa amenaza y estar preparado para ello.

4. **¿Conoce algún sistema que ayude a vigilar o detectar para neutralizar esta amenaza?**

   - Sí, el dispositivo tiene un sistema de localización y detección de la amenaza y en su caso poder neutralizar drones. Puede ser pesado o en una base puede ser fijo, y también puede ser portátil que lleve incorporado el operador con la mochila con todos los útiles necesarios.

5. **¿Cree que debería implantarse distintos tipos sistemas anti-drones debido a las incidencias últimas que ha habido con la amenaza de drones en Zona de Operaciones y/o Operaciones permanentes?**

   - Creo que los hay, están implantados, pero en áreas de exclusión como pueden ser bases o si se crea un despliegue semipermanente entre otras cosas se instalaría en los Puestos Mandos algún sistema anti-dron. Lo que destaca en zonas de operaciones es la inmediatez.

6. **¿Qué impacto tendría y en qué nos afectaría una amenaza de drones en Zonas de Operaciones y/o Operaciones permanentes?**

   - Involucrar mayor esfuerzo y capacidades dedicadas a la vigilancia y seguridad, incrementar más medios, más conocimientos y capacidades de ataque mediante medios improvisados como un IED,s que puede contener el dron. Sin embargo, lo normal en esas áreas de Operaciones nos enfrentamos contra terroristas y por tanto, esos drones como tal son de vigilancia. No tienen la dotación de ataque.

7. **¿Conoce los diferentes tipos de UAS que posee en Zona de operaciones y/o operaciones permanentes?**

   - Sí conozco van desde los micro-UAS,s hasta drones de tamaño estándar con una autonomía de hasta 10 kilómetros. Las mejores características son la emisión o captura de imágenes en tiempo real. Estos equipos mandan a la Unidad superior. Cada Unidad tienen su tipo de dron en función de su misión.

8. **¿Y los diferentes tipos de sistemas que tienen para detectar nuestros drones?**

- Desconozco las capacidades del enemigo, cuando fui al Líbano puede ser que haya algún equipo para la vigilancia de la base. En Irak teníamos drones pero solamente para observación del área de instrucción.

9. ¿Qué medidas adopta el ejército ante una amenaza de drones?

- Sistemas activos, fijos o portátiles para intervenir o combatir con Guerra Electrónica para inhabilitar los drones mediante un pulso electromagnético, normalmente son inhibidores que se encargan de neutralizarlos, pierdan su lectura y caigan.

10. ¿Qué medios conoce de UAS? ¿Cuenta en su orgánica con alguno?

- Los medios son los RAVEN. El Batallón tiene cedido los medios UAS, tenemos operadores.

11. ¿Le parece necesaria la adquisición de este tipo de medios a su nivel?

- Es necesaria la adquisición, amplía las necesidades de seguridad y de observación de cualquier tipo de Unidad sin tener que entrar en combate y exponer a sus fuerzas y por ello tampoco en ser descubierto.

12. ¿Debería el ejército implantar alguna Unidad en la cual se emplee diferentes tipos de sistemas anti-drones? ¿Por qué? Si es sí, ¿Cuáles cree?

- Para Sistemas anti-dron pienso que no debería implantarse, pero capacitar o dotar las Unidades con Sistema anti-dron, a las Brigadas o bajar a nivel Batallón, sí. Capacitarlos con sistemas portátiles, con uno o dos sistemas. Es muy importante, ya que cada vez se utiliza más los drones.

13. ¿Hay personal especializado, operadores de UAS y que tengan conocimientos sobre los tipos de sistemas anti-drones?

- No tenemos personal suficiente especializado en esto y por tanto nuestros medios están en Almería.

14. ¿Cuánto coste tienen invertido o qué consideran invertir para la implementación de sistemas para la protección de la frontera contra los UAS?

- Desconozco el coste invertido, tengo entendido que se está invirtiendo últimamente mucho en drones y sistemas anti-drones.

15. ¿Considera que se debería mejorar la tecnología para poder combatir contra esta amenaza?

- Sí, es muy importante mejorar sobre todo en este ámbito, de esta nueva tecnología, porque en unos años será lo imprescindible para evitar fines maliciosos.

16. ¿Cuenta con los medios suficientes para la mejora de la tecnología de drones?

- Aquí, no tenemos los medios suficientes, como ya he dicho, los materiales están en Almería donde hay una Unidad perteneciente a Melilla.

17. ¿Tienen drones contramedidas (*Hardkill*) para interceptar drones hostiles?

- Tengo entendido que se trata de un dron que se encarga de interceptar el dron enemigo, pero no disponemos de este tipo de sistema.