REPÚBLICA DE COLOMBIA
AUTORIDAD AERONÁUTICA DE AVIACIÓN DE ESTADO
FUERZA AÉREA COLOMBIANA

GUÍA

SISTEMAS CONTRA UAS (C-UAS)

Mayo 2024

GUÍA
SISTEMAS CONTRA UAS (C-UAS)

La presente Guía Sistemas Contra UAS (C-UAS) surge de la necesidad dividir los conceptos de Sistemas Aéreos No Tripulados (UAS) y Sistemas Contra UAS (C-UAS) contempladas en la Guía Sistemas Aéreos No Tripulados (UAS) y Sistemas Contra UAS (C-UAS) Versión 01 publicada en mayo de 2022 para así publicar Guías para cada concepto de manera independiente con la intensión de permitir a los EAE reconocer de manera práctica y sencilla estos sistemas por separado.

La Guía Sistemas Contra UAS (C-UAS) actualiza la información contenida en la Guía publicada en el 2022 e incorpora nuevos conceptos de planificación para el empleo de los sistemas C-UAS de acuerdo al estudio y análisis realizado a referencias internacionales de instituciones civiles y militares como la Organización de Aviación Civil Internacional (OACI) el U.S. ARMY, U.S. Air Force, entre otros.

La presente GUÍA se encuentra publicada en la página web:
https://aaaes.fac.mil.co/es/normatividad

Para realizar cualquier consulta referente a la presente Guía, favor dirigirse a la Oficina de Autoridad Aeronáutica de Aviación de Estado, ubicada en la Carrera 13 No. 66-47 oficina 203, comunicarse al teléfono +57 (601) 3159800 en la extensión 63000 o al correo institucional aaaes@fac.mil.co.

ENMIENDAS O CAMBIOS A LA GUÍA UAS/C-UAS

Enmienda Numero	Origen	Tema	Adoptada/Surte efecto
001	N/A	GUIA SISTEMAS AÉREOS NO TRIPULADOS (UAS) Y SISTEMAS CONTRA UAS (C-UAS) Versión 01	Mayo 2022
002	Surge de la necesidad dividir los conceptos de Sistemas de Aeronaves No Tripuladas y Sistemas Contra UAS	La Guía Sistemas Contra UAS (C-UAS) deroga el capítulo C de la Guía Sistemas Aéreos No Tripulados	Mayo 2024

	(C-UAS) y publicar Guías para cada concepto. Adicionalmente implementa procedimientos de planeamiento clave para el empleo de sistemas C-UAS	(UAS) Y SISTEMAS CONTRA UAS (C-UAS) Versión 01	

INTENCIONALMENTE EN BLANCO

TABLA DE CONTENIDO

INTENCIONALMENTE EN BLANCO

TABLA DE ILUSTRACIONES

INTENCIONALMENTE EN BLANCO

INTRODUCCIÓN

El presente documento constituye una Guía de conceptos y procedimientos diseñados para los Entes de Aviación de Estado (EAE). Propende actualizar los conceptos relacionados a los Sistemas Contra UAS (C-UAS), afianzar los conocimientos sobre generalidades y funcionamiento de los mismos en la Aviación de Estado (AE), advertir sobre los riesgos y amenazas inherentes al desarrollo tecnológico de la Aviación No Tripulada en el mundo y propender por el alcance de los más altos niveles de seguridad operacional para la AE.

Mediante la presente Guía, los EAE logrará realizar una aproximación a un Concepto Operacional para el empleo de los sistemas C-UAS con una planificación organizada para permitir un uso efectivo con reducción de presentar los riesgos asociados a su operación.

De otra parte, busca difundir a los EAE, información relevante sobre la operación de UAS y C-UAS de forma tal que su personal tenga herramientas para detectar oportunamente posibles usos ilícitos de esos sistemas y/o situaciones que pongan en riesgo la seguridad de las unidades militares y de policía, así como la afectación a personalidades que requieran ser protegidas contra estos elementos, con el fin que puedan actuar como parte integral del sistema de seguridad, realizar reportes oportunos de avistamiento y coadyuvar en el proceso de actuación, disuadir y, en el caso de ser estrictamente necesario, realizar la neutralización de una amenaza potencial o inminente. En dicho sentido, es necesario sensibilizar al personal de los EAE en todas sus cadenas de mando respecto de la necesidad de percibir esta amenaza como un reto tecnológico, que requiere disponer de sistemas C-UAS, procedimientos y estrategias organizacionales capaces de hacerle frente con eficacia y seguridad, evolucionando al ritmo que lo hacen los UAS LSS y gestionando correctamente las vulnerabilidades de los EAE.

Lo anterior, en observancia al artículo 8 del Convenio de Aviación Civil Internacional (Convenio de Chicago aprobado por el Congreso de Colombia con la Ley 12 de 1947) el cual establece respecto de las aeronaves sin piloto que *“(…) Cada Estado contratante se compromete a asegurar que los vuelos de tales aeronaves sin piloto en las regiones abiertas a la navegación de las aeronaves civiles sean controladas de forma que se evite todo peligro a las aeronaves civiles.”,* y en concordancia con el artículo 37 del citado Convenio el cual refiere que *“Cada Estado contratante se compromete a colaborar, a fin de lograr el más alto grado de uniformidad posible en las reglamentaciones, normas, procedimientos y organización relativos a las aeronaves, personal, aerovías y servicios auxiliares, en todas las cuestiones en que tal uniformidad facilite y mejore la navegación aérea.”.*

INTENCIONALMENTE EN BLANCO

CAPÍTULO A. DEFINICIONES, ABREVIATURAS Y REFERENCIAS

1. Definiciones

Las siguientes definiciones y abreviaturas aplican al contenido de la presente guía.

Aeronave no tripulada. Aeronave destinada a volar sin piloto a bordo.

Aeronave pilotada a distancia –RPA. "Aeronave no tripulada que es pilotada desde una estación de pilotaje a distancia por un Piloto remoto, emplazado en una estación de control ubicada fuera de la aeronave (es decir en tierra, en barco, en otra aeronave, en el espacio, entre otros)" (OACI, 2015).

Aeronavegabilidad. Estado de una aeronave, motor, hélice o pieza que se ajusta al diseño aprobado correspondiente y está en condiciones de operar de modo seguro.

Base de lanzamiento. Ubicación geográfica seleccionada por el EAE para el despegue y recuperación de sus UAS/RPAS, la cual puede o no, hacer parte de la infraestructura y/o terrenos de un aeródromo.

Clasificación de UAS amenaza: La clasificación es el proceso posterior a la identificación que permite determinar características específicas de una detección y fijar procedimientos.

Captura directa *(Snagging):* Método que permite la captura del UA a través del empleo de redes expulsadas desde otras aeronaves pilotadas remotamente o elementos ubicados en tierra.

Carga útil: Todos los elementos del UA/RPA que no son necesarios para volar pero que son transportados para el cumplimiento de una misión específica que tienen encomendada. La carga útil puede estar relacionada con vigilancia, armas, comunicaciones, detección aérea, o carga propiamente dicha.

Centro de Comando y Control: Hace referencia a la dependencia, oficina o entidad encargada de centralizar las comunicaciones y dirigir el flujo de comunicación en el aeródromo o zona restringida, para que los encargados tomen decisiones tendientes a proteger los recursos asignados.

Comunicaciones por enlace de datos. Forma de comunicación destinada al intercambio de mensajes mediante enlace de datos.

Contramedidas de UAS. Sistemas dotados con la capacidad de interrumpir, deshabilitar, destruir, tomar el control y/o proporcionar instrucciones de vuelo alternativas a un UAS objetivo.

Control Operacional. Autoridad ejercida respecto a la iniciación, continuación, desviación o terminación de un vuelo en interés de la seguridad de la aeronave y de la regularidad y eficacia del vuelo.

Cetrería. Técnica relacionada con la cría, amaestramiento y cuidado de aves rapaces para la casa de otras especies.

Dazzling. Empleo de un haz de luz de alta intensidad o láser para "cegar" el sensor del UA.

Despegue. Conjunto de maniobras que efectúa la aeronave para elevarse de la superficie y emprender el vuelo. La expresión “despegue” en este documento incluye catapultas, VTOL, lanzamiento manual, desplazamiento vertical, despegue desde pistas y cualquier otro modo de decolaje de los UAS/RPAS.

Detección de UAS. Es una declaración de que un UAS está en presencia de un sensor. Algunos sistemas, dependiendo de cómo estén configurados, pueden señalar cualquier objeto a su vista como detección (es decir, pájaros, aviones comerciales, entre otros.), o pueden alertar al operador únicamente de los objetos que se consideran UAS, basados en sus capacidades.

Dirección de Navegación Aérea. Dependencia de la Fuerza Aérea Colombiana proveedora de los servicios para la navegación aérea de la Aviación de Estado, encargada de dirigir y coordinar las actividades relacionadas con la navegación aérea militar y policial y la administración del espacio aéreo nacional.

Dron. Expresión popular para referirse a cualquier aeronave no tripulada.

Electroóptica. Es una rama de la ingeniería eléctrica y física de la materia que involucra componentes, dispositivos (por ejemplo, láseres, leds, guías de onda, entre otros.) y los sistemas que utilicen la propagación y la interacción de la luz con diversos materiales adaptados.

Espacio aéreo controlado. Espacio aéreo de dimensiones definidas dentro del cual se facilita servicio de control de tránsito aéreo, de conformidad con la clasificación del espacio aéreo.

Nota. – Espacio aéreo controlado es una expresión genérica que abarca las clases A, B, C, D y E del espacio aéreo ATS.

Espacio aéreo segregado. Espacio aéreo de dimensiones especificadas asignado a usuarios específicos para su uso exclusivo.

Estación de Control en Tierra (GCS). Estación en la cual el Operador dirige el vuelo de una aeronave no tripulada. “Puede variar desde un dispositivo manual hasta una estación con varias consolas. Puede estar emplazada en el interior o en el exterior; puede ser estacionaria o móvil (instalada en un vehículo/barco/aeronave)” (OACI, 2015).

Enlace de mando y control. (C2) Enlace de datos entre la aeronave pilotada a distancia y la estación de pilotaje a distancia para fines de dirección del vuelo.

Hacking. Búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes.

Identificación de UAS amenaza. Identificación es el proceso que permite determinar si una detección desconocida es amistosa u hostil y su producto es la clasificación.

Interferencia intencionada *(Jamming):* Interferencia producida deliberadamente por emisiones destinadas a hacer ininteligibles o falsear en todo o en parte una señal deseada.

Láser: Dispositivo óptico que genera un haz luminoso de una sola frecuencia, monocromático, coherente y muy intenso, mediante la estimulación eléctrica o térmica de los átomos, moléculas o iones de un material

Latencia: Tiempo que tarda en transmitirse un paquete dentro de la red, y es un factor clave en las conexiones a Internet.

***Low, Slow and Steady*:** UA de superficie radar equivalente reducida, baja firma infrarroja y/o acústica, vuelo a baja altura y velocidad.

Meaconing: Un sistema de recepción de señales de radio baliza que las retransmite en la misma frecuencia para confundir la navegación. Las estaciones de medición hacen que las aeronaves y estaciones terrestres obtengan datos imprecisos.

Mitigación de UAS: Describe los métodos utilizados para eliminar o reducir la amenaza que representa un UA. Estos métodos incluyen medios técnicos, como interferencia de RF o GNSS, suplantación / secuestro y ataque cinético.

Modo autónomo de vuelo: Configuración de vuelo que le permite al UAS/RPAS volar sin la intervención de un Piloto Remoto u Operador, ejecutando acciones basadas en información suministrada por algoritmos, sensores y software previamente programados en la aviónica del Sistema.

Nivel táctico. Es el nivel en el EAE que se encarga de ejecutar objetivos de menor impacto, pero que contribuyen a los fines de su misión constitucional. Hace referencia también al empleo de los recursos en ese nivel.

Operador UAS: Personal capacitado, calificado y entrenado para operar de manera segura una aeronave no tripulada de la Clase I-A y/o I-B, con la capacidad de cumplir las misiones típicas y operacionales de cada uno de los EAE.

Operador al Mando. Personal designado por el EAE para estar al mando y encargarse de la realización segura de un vuelo.

Peso máximo de despegue (*MTOW, Maximum Take off Weight*). Equivale al peso vacío de la aeronave + 100% de carga útil + 100% de su capacidad de combustible.

Operación de vuelo. Actividad o grupo de actividades ejecutadas durante el período de vuelo de un UAS/RPAS, que obedecen a las capacidades específicas de su diseño y designación.

Operación con visibilidad directa visual (VLOS). Operación en la cual la tripulación remota mantiene contacto visual directo con la aeronave para dirigir su vuelo y satisfacer las responsabilidades de separación y anticolisión (tomado de la Circular 328-AN/190).

Operación con visibilidad más allá de la línea de vista (BVLOS). Cuando ni el piloto a distancia ni los observadores RPA puedan mantener contacto visual directo sin ayudas con la RPA, las operaciones se consideran BVLOS. Los requisitos de equipo mínimo para apoyar las operaciones BVLOS aumentan considerablemente a medida que aumenta el alcance y la complejidad de tales operaciones, así como los costos involucrados en asegurar la solidez del enlace C2. Es fundamental contar con capacidad para detectar tránsito en conflicto u obstáculos y adoptar las medidas apropiadas.

Operador UAS. Personal capacitado, calificado y entrenado para operar de manera segura una aeronave no tripulada de la Clase I-A o I-B, con capacidad de cumplir las misiones típicas y operacionales de cada uno de los EAE o aplicaciones civiles.

Performance. Voz inglesa que, para efectos de este reglamento, hace referencia al rendimiento o desempeño de las UAS/RPAS o aeronave convencional.

Peso máximo de despegue (MTOW). Equivale al Peso vacío de la aeronave + 100% de carga útil + 100% de su capacidad de combustible.

Piloto Remoto. Persona designada y avalada por el EAE mediante certificado de habilidad para desempeñar funciones esenciales para la operación de una aeronave pilotada a distancia y para operar los controles de vuelo, según corresponda, durante el tiempo de vuelo.

Plan de Vuelo. Información especificada que, respecto a un vuelo proyectado o a parte de un vuelo de una aeronave, se somete a las dependencias de los Servicios de Tránsito Aéreo.

Plan de Vuelo ATS. Información detallada proporcionada al Servicio de Tránsito Aéreo (ATS), con relación a un vuelo proyectado o porción de un vuelo de una aeronave. El término “Plan de vuelo” es utilizado para comunicar información completa y variada de los elementos comprendidos en la descripción del Plan de Vuelo, cubriendo la totalidad de la ruta de un vuelo o información limitada requerida, cuando el propósito es obtener una autorización para una porción menor de un vuelo tal como atravesar una aerovía, despegar desde o aterrizar en un aeródromo determinado.

Nota. – *Los requisitos respecto al Plan de Vuelo se encuentran en las Secciones 91.210 a 91.230 del RACAE 91, Reglas de Vuelo y Operación. Cuando se emplea la expresión “formulario de Plan de Vuelo”, se refiere al modelo del formulario de Plan de Vuelo OACI que figura en el Apéndice 2 del Documento 4444 ATM/501, Gestión de Tránsito Aéreo”, decimocuarta edición (2001) de la OACI (véase RAC 15 – Servicios de Información Aeronáutica).*

Probabilidad de derribo (Pk). Es la probabilidad de derribo de un sistema de armas específico. Se mide en un rango entre 0 y 1, siendo 0 el 0 % de posibilidad de derribar un objetivo y 1 el 100 %. Depende de numerosos factores como la probabilidad de que

el armamento impacte contra el objetivo (Phit) o la probabilidad de detección de la amenaza (Pd) entre otros.

Radar. Es un sistema que usa ondas electromagnéticas para medir distancias, altitudes, direcciones y velocidades de objetos estáticos o móviles como aeronaves, barcos, vehículos motorizados, formaciones meteorológicas y el propio terreno. Su funcionamiento se basa en emitir un impulso de radio, que se refleja en el objetivo y se recibe típicamente en la misma posición del emisor. A partir de este "eco" se puede extraer gran cantidad de información. El uso de ondas electromagnéticas permite detectar objetos más allá del rango de otro tipo de emisiones. Entre sus ámbitos de aplicación se incluyen la meteorología, el control del tráfico aéreo y terrestre y gran variedad de usos militares.

Radiación Infrarroja (IR). Es un tipo de radiación electromagnética, de mayor longitud de onda que la luz visible, pero menor que la de las microondas. Consecuentemente, tiene menor frecuencia que la luz visible y mayor que las microondas. Su rango de longitudes de onda va desde unos 0,7 hasta los 1000 micrómetros.

Radiofrecuencia (RF). También denominado *espectro de radiofrecuencia* es un término que se aplica a la porción menos energética del espectro electromagnético, situada entre los 3 hercios (Hz) y 300 gigahercios (GHz).

Sistema aéreo no tripulado (*UAS, Unmanned Aerial System*). Aeronave y sus elementos asociados, la cual es operada sin piloto a bordo.

Sistema Contra UAS (C-UAS, *Counter Unmanned Aircraft System).* Conjunto de sistemas, integrados por sensores, sistema de mando y control (C2) y sistemas de armas que permiten la detección, identificación y neutralización de UAS.

Sistema de Aeronaves Pilotadas a Distancia (*RPAS: Remotely- Piloted Aircraft System).* Aeronave pilotada por un “Piloto Remoto”, ubicado en una estación remota localizada fuera de la aeronave (ejemplo: en tierra, barco, otra aeronave, en el espacio); quien monitorea la aeronave todo el tiempo y puede responder a las instrucciones de ATC, efectuar comunicaciones apropiadamente vía voz o enlace de datos de acuerdo a la operación o espacio aéreo, y es responsable por la conducción segura de la aeronave durante su vuelo. Comprende un conjunto de elementos configurables incluyendo una RPA, sus estaciones de piloto remoto conexas, los necesarios enlaces C2 y todo otro elemento del sistema que pueda necesitarse, en cualquier punto durante el vuelo. Otras características podrían comprender soporte lógico, vigilancia de la salud, equipo de comunicaciones ATC, sistema de determinación de vuelo y elementos de lanzamiento y recuperación (OACI, 2011).

Sistemas de Gestión de Tránsito Aéreo para UAS/RPAS (UTM: Unmanned Aircraft System Traffic Management). Es un ecosistema de "Gestión del Tráfico para operaciones no controladas que es independiente, pero complementario, del Sistema de Gestión del Tráfico Aéreo (ATM). El desarrollo de UTM finalmente identificará servicios, roles y responsabilidades, arquitectura de información, protocolos de intercambio de datos, funciones de software, infraestructura y requisitos de rendimiento para permitir la gestión de operaciones de drones no controlados a baja altitud.

Suplantación *(Spoofing).* Método que permite sustituir las señales de posicionamiento del UAS para hacer creer a la aeronave que se encuentra en una posición distinta a la real.

Telemetría. Sistema automatizado de comunicación (alámbrico o inalámbrico) que le permite al UAS/RPAS almacenar información, procesarla y trasmitirla hasta el lugar donde se monitorea y controla el sistema. Para esto, se requiere de varios sensores que miden magnitudes físicas, químicas, entre otras, y que transforman esta información en señales análogas o inalámbricas para su envío y procesamiento.

Ubicación de UAS. Es un informe o visualización estimada de dónde se encuentra una GCS o UAS en un momento dado.

VTOL (*Vertical Take-off and Landing*). Capacidad de ciertas aeronaves, tripuladas y no tripuladas, para efectuar las maniobras de despegue y aterrizaje de forma vertical, mientras que en vuelo recto y nivelado se utiliza el método de propulsión horizontal.

Zona de Operaciones Militares (*MOA-Military Operational Airspace*). Espacio aéreo de carácter temporal, de dimensiones definidas sobre el territorio o las aguas jurisdiccionales de un Estado, reservado para el vuelo de aeronaves en desarrollo de actividades de la Aviación de Estado. Se usa esta expresión cuando el vuelo de aeronaves de Estado, dentro del espacio aéreo designado, está condicionado a determinadas horas, bajo condiciones específicas y con la activación previa del SECOC en el COPAE. Los servicios de Control de Tránsito Aéreo al interior del área son suministrados por la dependencia de control que tenga responsabilidad sobre citado espacio aéreo.

Zona prohibida. Espacio aéreo de dimensiones definidas sobre el territorio o las aguas jurisdiccionales de un Estado, dentro del cual está prohibido el vuelo de las aeronaves.

Nota. - En la AIP de Aviación de Estado ENR 5.1, se establece que las Zonas Prohibidas son un Espacio Aéreo administrado y controlado por la Fuerza Aérea.

Zona restringida. Espacio aéreo de dimensiones definidas sobre el territorio o las aguas jurisdiccionales de un Estado, dentro del cual está restringido el vuelo de las aeronaves, de acuerdo con determinadas condiciones especificadas.

Nota. - En la AIP de Aviación de Estado ENR 5.1, se establece que las Zonas Restringidas son un Espacio Aéreo administrado y controlado por la Fuerza Aérea.

2. Abreviaturas

AAAES. Autoridad Aeronáutica de Aviación de Estado.

AE. Aviación de Estado.

BVLOS. *Beyond Visual Line of Sight.*

DA. Defensa Aérea.

EAE. Ente de Aviación de Estado.

EO. Electroóptico.

IR. Infrarrojo.

LSS. *Low, Slow and Steady.*

MOA. *Military Operational Airspace.*

MTOW. *Maximum Take off Weight*

NBQR: Nuclear, Biológico, Químico, Radioactivo.

UA. *Unmanned Aircraft.* Aeronave no tripulada.

UAS. *Unmanned Aerial System*. Sistema Aéreo no Tripulado.

UAV. *Unmanned Aerial Vehicle*. Vehículo Aéreo no Tripulado (Termino en desuso, OACI 2015).

VTOL. *Vertical Take-off and Landing***.**

3. Referencias

- Austin, R (2010). *Unmanned Aircraft Systems, UAV design, development and deployment*. Wiley.
- Autoridad Aeronáutica de Aviación de Estado (2019), *Circular Informativa No. 003-19 Funcionamiento y Generalidades Sistema No Tripulado*, Bogotá- Colombia.
- Autoridad Aeronáutica Aviación de Estado (2022), RACAE 94 Reglas De Vuelo Y Operación Para Sistemas Aéreos No Tripulados Y Sistemas De Aeronaves Remotamente Pilotadas, Enmienda 1.
- Barnhart, Hottman, Marshall, Shappee (2012). *Introduction to Unmanned Aircraft Systems*. CRC Press.
- Department of the Army (2023), ATP 3-01.81, Counter-Unmanned Aircraft System (C-UAS).
- FAA *(2019), Unmanned Aircraft System Detection-Technical Considerations.*
- Ministerio de Defensa de España (2019), *Concepto Nacional C-UAS LSS*, Centro Conjunto de Desarrollo de Conceptos, Madrid-España.
- Ministerio de Defensa de España (2018), *GT Tecnología- Concepto Contra Sistemas Aéreos No Tripulados*, Centro Conjunto de Desarrollo de Conceptos, Madrid-España.

- *Michel (2019), Counter-drone Systems*
- OACI (2011), Circular 328 AN/190, *Sistemas de Aeronaves No Tripuladas (UAS).*
- OACI (2015), Doc. 10019 AN/507, *Manual sobre Sistemas de Aeronaves Pilotadas a Distancia (RPAS).*
- *Olsen, J. A. (2017). Warden Revisited: The Pursuit of Victory Through Air Power. Air Power History, 64(4), 39-53.*
- United Nations Human Rights (septiembre, 1990), Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.
- U.S Air Force (junio, 2015), Air Force Doctrine Publications 3.01 Counterair Operations.
- U.S Air Force (septiembre, 2021), Air Force Doctrine Publications 3.60 Targeting.

INTENCIONALMENTE EN BLANCO

CAPÍTULO B. LOS SISTEMAS DE AERONAVES NO TRIPULADAS COMO AMENAZA

1. Antecedentes empleo UAS como amenaza

El desarrollo exponencial de las tecnologías de uso recreativo o entretenimiento aplicadas al sector de los UAS; la creciente oferta en el mercado, bajo costo, simplicidad, entre otros factores que facilitan su adquisición, merman las capacidades de aplicación de medidas de control de las entidades estatales para la adquisición y operación por parte de particulares de los UAS. Como resultado, presenciamos en la actualidad un cambio significativo en el entorno operacional tanto en el ámbito de la aeronáutica como en el ámbito de seguridad pública y militar.

Dentro de los eventos objeto de referencia de este capítulo, son relevantes las intrusiones de Aeronaves No Tripuladas (UA), en aeropuertos de alto flujo operacional como Singapur, Frankfurt, Dublín, Madrid y Londres, situaciones que han resultado en el cierre de sus pistas, paralizando las operaciones aéreas, ocasionado el retraso y cancelación de vuelos programados y generando grandes pérdidas, tanto para las empresas operadoras como para los usuarios, además de riesgos considerables para la seguridad de las aeronaves tripuladas. Así mismo, los eventos operacionales por intrusión de UA en diferentes Aeropuertos de Colombia, especialmente en el Aeropuerto Internacional “El Dorado” de Bogotá y los avistamientos de sistemas de este tipo en las inmediaciones de las Unidades Militares, de Policía y algunas edificaciones consideradas infraestructura crítica de la Nación.

Como ejemplo de amenaza a la seguridad, en agosto de 2018 fueron reportados por las autoridades venezolanas dos UA DJI M600 que transportaban un kilogramo de C4 cada uno, con la intensión de atentar contra el presidente Nicolás Maduro en Caracas mientras realizaba un discurso. El atentado no se produjo, pero se conoció como uno de los primeros intentos de atentado contra un jefe de estado mediante el empleo de estas aeronaves.

El ataque perpetrado el 15 de septiembre de 2019 contra las instalaciones de 2 refinerías de la empresa saudí ARAMCO, responsable de la producción de un alto porcentaje del Petróleo mundial y para lo cual se emplearon 18 Aeronaves No Tripulados y 7 misiles de crucero.

En Colombia, en el mes de abril de 2024, la Fuerza Pública descubrió en el departamento del Cauca un depósito ilegal de artefactos explosivos debidamente acondicionados para ser lanzados desde Aeronaves No Tripuladas. De acuerdo a lo expuesto por las entidades del estado, estos explosivos serían empleados para atentar contra infraestructura crítica del país y personal uniformado de la Fuerza Pública. Algunos meses antes, circuló por redes sociales un video aparentemente realizado desde una UA desde la cual se arrojan artefactos que explotan al impactar con el terreno

Por lo anterior, es de suma importancia considerar que los Entes de Aviación de Estado (EAE) actualmente tienen el riesgo de ser afectados por Aeronaves No Tripuladas en el ámbito regular o no regular y, en consecuencia, alterar el normal desarrollo de sus

operaciones y actividades.

2. Categorización de la amenaza

Existen múltiples clasificaciones y categorías de UAS en función del peso, altitud de vuelo, alcance, nivel de empleo, entre otras, pero en general, las diferentes clases de Sistemas Aéreos No Tripulados (UAS) se establecen en relación con el peso máximo de despegue (*MTOW, Maximum Take off Weight)*.

Sin embargo, debido a la proliferación exponencial, cuantitativa y cualitativa, de los UAS y la amplitud del espectro para su modificación, algunas de estas clasificaciones se consideran un tanto decimonónicas y, en este sentido, resulta un desafío establecer una categorización de la amenaza que sea perdurable y que no esté sujeta a constantes actualizaciones.

Ilustración 1: Categorización de amenaza

	UAS CLASE IA	UAS CLASE IB	RPAS CLASE IC Y ID
			
Peso	200 g a <7 Kg	7kg a <15 Kg	15Kg a < 80 Kg
Altitud	<400 pies AGL	<1000 pies AGL*	>15000 pies AGL
Velocidad	Hasta 40 Kts	Hasta 50 kts	Hasta 80 Kts
Autonomía	<40 minutos	3-4 horas	>16 horas

*La altitud de operación de los UAS de la Aviación de Estado es de 400 pies AGL en espacios aéreos Clase G.

Fuente: Construcción AAAES.

Por lo tanto, para efectos de este capítulo, la categorización de la amenaza "*se enfocará en aquellos sistemas que, debido a sus características de reducida superficie radar equivalente, baja firma infrarroja y/o acústica, o vuelo a baja altura y velocidad, denominados UAS LSS, hacen que se sitúen fuera de la envolvente de detección, seguimiento, identificación y neutralización de los sistemas actuales de Defensa Aérea (DA)"* (Centro Conjunto de Desarrollo de Conceptos, 2019), ocasionando que los medios disponibles para la DA y Protección de los EAE no resulten eficaces.

Por lo anterior, se consideran tres escenarios fundamentales:

- **Unidades e instalaciones militares en operaciones transitorias.** Incluye las Unidades a flote, fuerzas desplegadas y demás Unidades militares y de policía móviles sobre las cuales se proyecta una amenaza creciente debido a la evolución del empleo

hostil de UAS LSS, desde su utilización como sensores de vigilancia de la actividad propia, hasta el uso como vector de armamento improvisado.

- **Unidades e instalaciones militares fijas.** En este tipo de unidades militares y de policía, factores tales como el entorno urbano, la presencia de población civil, la proliferación del uso recreativo de estos sistemas, la posible vulnerabilidad de las infraestructuras críticas y la alarma social que podría provocar esta Amenaza en territorio nacional, implican una mayor complejidad y la aparición de nuevos aspectos a considerar.

- **Personalidades en ubicaciones temporales.** Se consideran a las personalidades de altos cargos públicos de la República de Colombia o de otros países que, en ejercicio de sus funciones, deben desplazarse entre diferentes ubicaciones y, por lo tanto, su seguridad debe ser defendida.

3. Sistemas de Sensores como amenaza

Los sensores son todos los elementos del UA/RPA que no son necesarios para volar pero que son transportados para el cumplimiento de una misión específica que la aeronave tiene encomendada. Los sensores pueden estar relacionados con vigilancia, comunicaciones, detección aérea, entre otros.

Estos elementos, se consideran una potencial amenaza dado a que, sumando las capacidades y características de la Aeronaves No Tripuladas, permiten realizar vigilancia, inteligencia, recopilación de datos importantes e incluso emplearlos con el propósito de hacer más preciso el armamento o la conducción de acciones en contra de la seguridad.

Los tipos de sensores son activos y pasivos. Los sensores pasivos, reciben perturbaciones ya existentes del campo electromagnético y por medio de diferentes herramientas de hardware y/o software transforman estas perturbaciones en datos como imágenes digitales o radiofrecuencias. Normalmente los sensores activos funcionan dentro de las frecuencias de luz visible y cercanas a la infrarroja. Los sensores activos, a diferencia de los pasivos, emiten su propia perturbación electromagnética y por efecto Doppler, al retornar a sus receptores de ondas electromagnéticas transforman estas perturbaciones en datos legibles. Algunos ejemplos de sensores activos son radares, LiDAR o sensores sonar.

Los sensores más comúnmente empleados en las Aeronaves No Tripuladas por su baja complejidad, eficaces y confiables son los sensores visuales o electroópticos, es decir, que son sensores pasivos que funcionan mediante las ondas electromagnéticas emitidas por una fuente de radiación externa dentro del rango de la luz visible (el sol es el más común). En consecuencia, gran parte de los esfuerzos para evitar esta amenaza deben estar enfocados en el empleo de técnicas y tácticas que distorsionen o disminuyan la detección de los activos a proteger por medio de estos tipos sensores. En la Sección 2. Medidas Pasivas del capítulo E se ampliará la información referente a las técnicas y tácticas que reducen la efectividad de estos sensores.

Otros sensores empleados por los UAS son los sensores con capacidad de onda infrarroja o cercana a la infrarroja. Aunque son más complejos y costosos, permiten la operación nocturna, con bajas condiciones de visibilidad y poseen la capacidad de detectar emisiones

de calor. De la misma manera, para contrarrestar la amenaza proveniente de este tipo de sensores, se deben tener en cuenta las técnicas y tácticas de la Sección 2 Medidas Pasivas del capítulo E de la presente Guía.

INTENCIONALMENTE EN BLANCO

CAPÍTULO C. SISTEMAS CONTRA UAS (C-UAS)

1. Definición Sistemas C UAS

La *Tecnología de contraataque* (Michel, 2019), también conocida como contra-UAS o simplemente C-UAS, se refiere a sistemas que se utilizan para detectar y/o deshabilitar Aeronaves No Tripuladas o a alguno de los componentes de sus sistemas (Antenas de transmisión, Antenas GPS, que no están a bordo de la aeronave). Es un *"sistema de sistemas"* formado por diferentes sensores, interfaces de mando y control (C2) y sistemas de armas, diseñados para las diferentes fases de lo que se denomina *Ciclo C-UAS.*

2. Clasificación C-UAS

2.1. Tipos de tecnología C-UAS

Si bien, la oferta tecnológica de C-UAS en el mundo es difícil de dimensionar, es posible categorizarla en dos grupos: Cinética y No cinética.

La ***tecnología cinética*** es representada por los sistemas de DA actuales (Ej.: Sistemas Patriot, F-100, NASAMS, HAWK, Misil Mistral, entre otros), mientras que la ***tecnología No cinética*** puede sub-clasificarse en sistemas de detección, seguimiento e identificación (medios pasivos) y sistemas de mitigación (medios reactivos).

2.2 Sistemas de Defensa Aérea y sus limitaciones

Los Sistemas de Defensa Aérea actuales emplean mayoritariamente sistemas de armas cinéticos para neutralizar amenazas aéreas, los cuales son totalmente válidos para amenazas convencionales, por ejemplo, RPAS de categorías II y III, debido a su similitud a las aeronaves tripuladas por su envergadura. Sin embargo, su utilización frente a UA de categoría I, tipo MICRO y MINI o UAS LSS presenta una serie de limitaciones que deben ser evaluadas. Entre estas limitaciones es posible destacar:

(a) **Daño colateral:** La neutralización de Aeronaves No Tripuladas LSS por medio de sistemas de armas cinéticos en entornos urbanos puede ir en contra del daño colateral aceptable, por lo que su uso puede estar restringido. Los daños colaterales y afectaciones a terceros deberán ser reportados a las dependencias encargadas de cada institución para realizar los procedimientos administrativos pertinentes de reparación.

(b) **Economía:** Los costos de empleo del armamento de los Sistemas de DA frente a un enemigo convencional son relativamente equilibrados y en muchos casos beneficiosos, por lo que su operación es asumible y justificable. Sin embargo, dado el bajo costo de los UAS LSS, emplear este tipo de sistemas para su neutralización resulta poco factible.

(c) **Cantidad:** Actualmente ningún sistema de armas cinético puede hacer frente a un ataque masivo de UAS y, en el caso de que pudiera hacerle frente, el costo económico y de material sería inasumible.

(d) **Efectividad:** Para los sistemas de armas cinéticos, un objetivo UAS LSS supone un verdadero reto por sus características especiales, por lo que la probabilidad de derribo (Pk) esperada frente a esta amenaza podría ser en algunos casos elevada y en otros prácticamente nula, dependiendo del perfil de vuelo del objetivo, así como de diversos condicionantes.

2.3. Sistemas de detección, seguimiento e identificación

Se encargan de identificar las señales del UAS, determinar su ubicación y, en algunos casos, un vector hacia su punto de control.

Dentro de estos sistemas encontramos los radares, receptores de ondas de radio, sensores acústicos y sensores ópticos, cuyas características son:

INTENCIONALMENTE EN BLANCO

Tabla 1: *Sistemas C-UAS de detección, seguimiento e identificación*

TIPO DE SISTEMA	DESCRIPCIÓN
Radar	Detecta la presencia de UAS LSS por su firma de radar, generada cuando la aeronave encuentra pulsos de radiofrecuencia emitidos por el elemento de detección. Estos sistemas a menudo emplean algoritmos para distinguir entre UAS y otros objetos pequeños, como pájaros.
Radio-Frecuencia	Detecta, localiza y, en algunos casos, identifica UAS cercanos escaneando las frecuencias en las que se sabe que operan la mayoría de estos.
Electro-óptico (EO)	Identifica y rastrea UAS en función de su firma visual.
Infrarrojo (IR)	Identifica y rastrea UAS en función de su firma de calor.
Acústico	Detecta UAS al reconocer los sonidos únicos producidos por sus motores. Se basan en una biblioteca de sonidos producidos por UAS conocidos, que luego se comparan con sonidos detectados en el entorno operativo.
Sensores Combinados	Muchos sistemas integran una variedad de diferentes tipos de sensores para proporcionar una mayor capacidad de detección, seguimiento e identificación.
Cetrería	Adiestramiento de aves rapaces para la captura o interceptación de UAS en vuelo.

Fuente: Michel (2019), Counter-drone Systems

Los sistemas basados en radar se pueden usar como un medio principal de detección; sin embargo, generalmente se enfrentan a la falta de automatización y dependen en gran medida de un operador capacitado para darse cuenta de identificaciones nuevas o cambiantes, trazar y rastrear geolocalizaciones, y elegir la configuración de sistema adecuada.

Este tipo de sistemas también enfrenta dificultades cuando se emplean con UAS que solo se mueven verticalmente o se desplazan en su lugar. Algunos sistemas radar pueden activar un sistema electroóptico secundario que apunta los sensores ópticos automáticamente en la dirección del objetivo de interés detectado. Esta característica puede ser inefectiva, en ocasiones, si el sistema detecta inadvertidamente un avión tripulado más grande como un nuevo objetivo.

Los sensores de radar están especialmente ajustados para identificar objetivos pequeños a distancias cortas, medias o largas; por lo tanto, pueden ser necesarios múltiples radares con diferentes rangos de detección para cubrir las áreas objetivo.

Así mismo, los sensores electroópticos (EO) e infrarrojos (IR) no suelen servir como sistemas de detección primarios para identificar y rastrear un UAS. Sin embargo, pueden ser herramientas secundarias importantes de validación visual para objetivos detectados por sensores primarios. Aunque hay sistemas EO avanzados, que pueden proporcionar la capacidad de hacer seguimiento automático a imágenes de objetivos potenciales detectados; son vulnerables ante la posibilidad de ser redirigidos a objetivos falsos, como pájaros o aviones tripulados que cruzan el campo de visión.

2.4. Sistemas de mitigación

Son sistemas dotados con la capacidad de interferir con la señal de control entre el UAS y su operador, afectar el rendimiento del mismo, neutralizarlo e incluso suplantar su señal de control con el fin de detener cualquier actividad que realice. Algunos ejemplos de este tipo de tecnología son:

INTENCIONALMENTE EN BLANCO

Tabla 2: *Sistemas C-UAS de mitigación*

TIPO DE SISTEMA	DESCRIPCIÓN
Jamming de RF	Interrumpe el enlace de radiofrecuencia entre el UAS y su operador al generar grandes volúmenes de interferencia en la RF. Una vez que se corta el enlace RF, que puede incluir enlaces WiFi, el UAS generalmente descenderá al terreno o iniciará una maniobra de "regreso a casa".
Jamming de GNSS	Interrumpe el enlace satelital que el UAS utiliza para la navegación, como GPS o GLONASS. Los UAS que pierden su enlace satelital generalmente mantienen su posición actual, aterrizan o regresan al punto de control, lo cual facilita la identificación de la ubicación del operador.
Spoofing y/o Meaconing	Permiten suplantar las señales de posicionamiento del UAS para hacer creer a la aeronave que se encuentra en una posición distinta a la real, ocasionado errores en la ejecución de los comandos programados por el Operador.
Dazzling	Emplea un haz de luz de alta intensidad o láser para "cegar" la cámara del UAS.
Láser	Destruye segmentos vitales de la aviónica del UAS usando energía dirigida, lo que hace que impacte contra el terreno.
Microondas de alta potencia	Dirige pulsos de energía de microondas de alta intensidad al UAS, deshabilitando los sistemas electrónicos de la aeronave.
Snagging	Redes expulsadas desde otras aeronaves pilotadas remotamente o elementos ubicados en tierra con el fin de capturar al UAS en vuelo y obligarlo a aterrizar de manera controlada.
UAS de colisión	UAS diseñados para colisionar directamente contra otros clasificados como adversarios.
Hacking	Empleo de software malicioso que ataca las vulnerabilidades de seguridad en sistemas o redes necesarios para la operación del UAS, afectando su rendimiento.

Fuente: Michel (2019), Counter-drone Systems

Es de considerar que los fabricantes o vendedores de C-UAS usualmente ofrecen equipos que pueden operarse tanto en modo pasivo como activo, lo cual, en teoría, garantiza que únicamente interferirán en el rendimiento de las señales de Radio Frecuencia (RF) empleadas en la operación aérea cuando se tenga la intención de neutralizar un UA/UAS

catalogado como hostil. Sin embargo, se debe tener en cuenta que algunos sistemas pueden emitir señales durante los procesos de actualización de su software, la instalación del equipo en el sitio o durante las calibraciones del sistema. Por esta razón, no es posible asumir categóricamente que el sistema de detección emite energía de RF de forma completamente controlada lo cual puede representar un riesgo para la Seguridad Operacional.

Nota 2: *Consulte las capacidades, limitaciones, ventajas y desventajas de los Sistemas C-UAS más utilizados en el Anexo 1 de esta Guía "Características y limitaciones del Sistemas C-UAS de mayor empleo".*

2.5. Tipos de plataformas C-UAS

Existen diferentes tipos de plataformas C-UAS entre las que destacan las 3 siguientes:

a) **Instalados en tierra (ground-based):** Son sistemas diseñados para ser utilizados desde una estación fija o móvil en tierra, esta categoría incluye sistemas instalados en sitios fijos, sistemas móviles, y sistemas montados en vehículos móviles.

b) **Portátiles o de mano (Hand-held):** Sistemas que son diseñados para ser operados por una persona o por sistemas automatizados muy simples que no requieren grandes infraestructuras, muchos de estos sistemas se asemejan a rifles u otras armas pequeñas.

c) **Instalados en UA:** Sistemas diseñados para ser instalados en un UA los cuales pueden estar en las proximidades del objetivo con el fin de emplear una interdicción la Aeronave No Tripulada enemiga intentando realizar un cerramiento del rango de operación.

INTENCIONALMENTE EN BLANCO

CAPÍTULO D. GUIA DE PLANEAMIENTO PARA EMPLEO C-UAS

1. Introducción

La guía establece una propuesta a los EAE para prevenir la amenaza generada por los Sistemas de Aeronaves No Tripuladas que pudieran llegar a generar una afectación al normal desarrollo de actividades de los EAE. Debido al incremento evidente de UAS en el contexto actual, es un escenario que debe ser afrontado por todos los niveles de mando de los Entes de Aviación de Estado. La efectividad de los C-UAS depende de la unificación de esfuerzos de diferentes actores dentro de los EAE. En consecuencia, la seguridad física depende de cada miembro de las instituciones.

Es importante precisar que la amenaza con Sistemas de Aeronaves No Tripuladas no se hace efectiva únicamente mientras la aeronave se encuentra en vuelo, la amenaza inicia desde mucho antes, incluso desde la preparación para ponerla en el aire. Por lo que es indispensable el análisis predictivo por medio de la inteligencia disponible y asimismo involucrar estos actores en los organismos de seguridad para contrarrestar la amenaza UAS.

Cada cadena del mando contribuye a la supervivencia creando Zonas de Alerta. Las Zonas de Alerta se componen de medidas pasivas y medidas activas que previenen la amenaza de los UAS alertando, ubicando o destruyendo el objetivo. Cada medida empleada para enfrentar la amenaza hace más compleja la materialización del riesgo.

2. Consideraciones para el planeamiento

El planeamiento es el primer paso para asegurar la efectividad de los C-UAS ante alguna amenaza. Neutralizar las amenazas requiere el empleo de diferentes componentes y capacidades y sincroniza sus actividades en toda la cadena de mando.

Para desarrollar un planeamiento coherente los EAE como mínimo deben establecer la siguiente estructura:

- Plan de Zonas de Alerta
- Reglas de Enfrentamiento
- Plan de Control del Espacio Aéreo
- Plan de Niveles de alerta
- Plan de Estado de Control de Armas
- Plan de Red de Alerta Temprana
- Plan de Lista de Protección Priorizada (PPL)

2.1. Plan de Zonas de Alerta

Las Zonas de Alerta proponen dar oportunidades para enfrentar amenazas a un rango máximo de distancia del objetivo a proteger. Los Niveles de Alerta se soportan por una distancia suficiente, alertas tempranas y activos de seguimiento.

El Plan de Control de Espacio Aéreo y el plan de Defensa Aérea deben incluir procedimientos detallados que permitan detectar, identificar, tomar decisiones y enfrentar la amenaza de manera oportuna ya que debido al aumento del empleo de UAS en diferentes organismos estatales y en los EAE para diferentes propósitos se dificulta la tarea de identificar si una UA hace parte de una amenaza o no. Pocos UAS cuentan con sistemas de identificación *identify-friend-from-foe (IFF)* o similares, que permitan descartar una amenaza real. Además, las características de la mayoría de las UA son similares (características físicas, tamaño, sonidos, entre otros), por lo cual se debe hacer un mayor esfuerzo para identificar la procedencia o intensiones de un UA.

La artillería de defensa aérea aplica siete principios para ejercer una defensa por zonas que puede emplearse para la organización de los sistemas C-UAS; soporte mutuo, fuegos superpuestos y coberturas superpuestas, fuegos equilibrados, cobertura equilibrada, cobertura temprana, defensa en profundidad y resiliencia.

2.1.1. Soporte mutuo

Las capacidades C-UAS están posicionadas de manera que el seguimiento o enfrentamiento a objetivos puede realizarse dentro de las zonas *Kill Zone* de otros sistemas C-UAS. El apoyo mutuo también puede cubrir sistemas C-UAS no operativos o sistemas en un estado de preparación.

2.1.2 Fuegos superpuestos y coberturas superpuestas

Las capacidades C-UAS se posicionan de manera que sus rangos de acción son superpuestos. Debido a la variedad de altitudes, alcances y velocidades de la amenaza aérea los rangos superpuestos permiten una mejor defensa de los objetivos a proteger. Esta ubicación superpuesta puede ser vertical como horizontal. La cobertura superpuesta también garantiza que los sensores C-UAS estén ubicados de manera que su cobertura no deje ninguna brecha en la defensa que pudiera ser utilizada para vulnerar la defensa.

2.1.3. Fuego equilibrado

Las armas C-UAS se posicionan para realizar un volumen igual de acción cinética o no cinética en todas direcciones. Esto es necesario en caso de que la dirección o ruta de la amenaza UA no es evidente.

2.1.4. Cobertura equilibrada

Las capacidades de los C-UAS se combinan y concentran hacia las vías aéreas de aproximación más probables. Las vías de aproximación pueden ser impredecibles, por lo que la cobertura equilibrada puede enfocarse en sectores o activos críticos.

2.1.5. Cobertura temprana

Las capacidades de los C-UAS están posicionadas de manera que pueden enfrentar la amenaza antes del despliegue de armas cinéticas o la adquisición de objetivos amigos. El enfrentamiento temprano permite la destrucción de plataformas enemigas fuera del territorio propio o en áreas desocupadas, reduciendo así la posibilidad de daños colaterales o fratricidio.

2.1.6. Defensa en profundidad

Las capacidades de los C-UAS están posicionadas de manera que la amenaza esté expuesta a un número cada vez mayor de efectos a medida que se acerca al activo u objetivo a defender. La defensa en profundidad disminuye la probabilidad de que los UAS atacantes alcancen el activo o la fuerza defendida.

2.1.7. Resiliencia

La resiliencia es la cualidad de la defensa para mantener la continuidad de las operaciones independientemente de los cambios de tácticas empleadas por parte del enemigo o la pérdida de capacidades de los C-UAS. Los líderes deben comprenden las capacidades de sus equipos C-UAS y actuar con agilidad para reasignar rápidamente capacidades según sea necesario.

2.2. Reglas de Enfrentamiento (ROE)

Los comandantes tienen la responsabilidad de tomar todas las medidas necesarias para proteger sus fuerzas y equipos contra ataques y garantizar que su personal opere de acuerdo con las Reglas De Enfrentamiento (ROE) establecidas.

Las Reglas de Enfrentamiento son directrices en las que se enmarcan las circunstancias y limitaciones bajo las cuales las fuerzas de una organización iniciarán o continuarán el enfrentamiento en contra de una amenaza. Las Reglas de Enfrentamiento deben adaptarse a deben adoptarse de acuerdo a Principios Básicos de Empleo De La Fuerza de Naciones Unidas de Derechos Humanos (ONU):

2.2.1. La legalidad.

Se refiere a adoptar las leyes y regulaciones sobre el uso de la fuerza.

2.2.2. Necesidad.

El uso de la fuerza está limitado a su empleo cuando sea estrictamente necesario, para obtener un legítimo objetivo. El uso de la fuerza solo es justificado como último recurso en casos de defensa propia, defensa de terceros ante una amenaza inminente de muerte o lesión, la prevención de un crimen con riesgo para la vida de otras personas, o la captura de sujetos potencialmente peligrosos.

2.2.3. Proporcionalidad.

Hace referencia a la limitación del potencial daño que pueda causar y deben ser estrictamente proporcionales a la gravedad de la falta y la legitimidad del objetivo a alcanzar.

2.2.4. Precaución.

Las operaciones deben ser planificadas de modo que se reduzca el uso indiscriminado de la fuerza para minimizar el riesgo para las personas que no están relacionadas con las operaciones. Para el caso de las Aeronaves No Tripuladas, se debe considerar incluso, que el uso de armamento no cinético no cause que la aeronave pierda el control y colisione de manera tal que genere daños considerables.

2.2.5. Rendición de cuentas.

Con el fin de demostrar la trasparencia de las operaciones, cuando el uso de la fuerza ocasiona muerte o lesiones, debe reportarse a la mayor brevedad. Estas acciones pueden generar investigaciones o incluso sanciones por el uso indebido de la fuerza.

El proceso de planeamiento, para la conducción de medidas C-UAS concibe un proceso lógico de ejecución, asignación de medios y determinación de misiones. Cada nivel se define por el objetivo a alcanzar.

Tabla 3: *Niveles de Defensa y Conducción*

Objetivos Estratégicos	Nivel Político y Comandantes de Fuerza	Decidir los objetivos a defender y proporcionar disuasión y seguridad en el marco de la Defensa Aérea (C-UAS). Su activación es una de las primeras medidas a tomar para responder a una crisis e incrementar los niveles de seguridad.
Objetivos Operacionales	Comandante de Área de Defensa	Contribuir a la integración de la Defensa Aérea (C-UAS) para la protección de las fuerzas y objetivos de interés.
Objetivos Tácticos	Coordinador de Defensa Aérea	Proteger fuerzas y objetivos de interés de niveles superiores y los que se le asignen de acuerdo a las prioridades. Presentar propuestas de empleo de la Defensa Aérea

		(C-UAS) de la organización operativa a la que se le protege.

2.3. Plan de Control del Espacio Aéreo

Las unidades distribuyen la orden de coordinación del espacio aéreo (conocida como *Airspace Coordination Order*, ACO), el plan del espacio aéreo de la unidad y la imagen aérea actual vertical a través de sistemas de comando y control a los que tienen acceso las unidades subordinadas. Las unidades subordinadas sin dependencias de defensa aérea, de gestión de tráfico aéreo o que no tengan acceso a estos sistemas, no tienen la capacidad de mantener una información actualizada del panorama aéreo y dependen de otras dependencias con esos sistemas para compartir y crear una alerta situacional apropiada.

El Plan de Control Aéreo debe adoptarse de acuerdo a la distribución del espacio aéreo en donde se esté operando. Debe realizarse un análisis de las zonas restringidas, prohibidas o peligrosas, MOA o espacios aéreos segregados o no segregados, A, B, C, D o G) ya que permite identificar el tipo de tráfico aéreo del área y sus respectivas dependencias de control.

2.4. Plan de Niveles de Alerta

El Plan de Niveles de Alerta (*Air Defence Warning, ADW*) es una advertencia de Defensa Aérea que se da en forma de código de color correspondiente al grado de probabilidad de amenaza aérea. Las condiciones de advertencia son un control de procedimiento utilizado para preparar las unidades en función de la amenaza evaluada. Se pueden proporcionar diferentes condiciones para diferentes amenazas aéreas. Las unidades subordinadas pueden disponer de condiciones más altas, pero no más bajas, para el área asignada. Es indispensable que todo el personal de la unidad conozca la condición de advertencia actual.

Hay tres tipos de ADW: rojo, amarillo y blanco, siendo el rojo el más urgente:

- ADW rojo. Un ataque con aeronaves o misiles hostiles es inminente o está en curso. (El estado de control de armas es **Sistemas C-UAS sin limitación**).

- ADW ambar. Es probable que se produzca un ataque con aviones o misiles hostiles (El estado de control de armas es **Sistemas C-UAS listos**).

- ADW amarillo. Un ataque con aviones o misiles hostiles es improbable (El estado de control de armas es **Sistemas C-UAS en reserva**).

2.5. Estado de control de armas

El estado de control de armas es una medida de control que establece las condiciones bajo las cuales se permite que las armas de defensa aérea (cinéticas y no cinéticas) enfrenten amenazas. La situación táctica normalmente determina el grado o extensión

del control necesario sobre sistemas de armas particulares. Los tres estados de control de armas para los C-UAS son:

- **Sistemas C-UAS sin limitación**. Enfrentar a cualquier UAS que no esté positivamente identificado de acuerdo con las ROE como amigable. Este es el estado de control de armas menos restrictivo.

- **Sistemas C-UAS listos**. Enfrentar únicamente UAS identificados como hostiles de acuerdo con las ROE.

- **Sistemas C-UAS en reserva**. Las unidades pueden accionar los sistemas C-UAS sólo en defensa propia o cuando lo ordene una autoridad superior adecuada. Este es el estado de control de armas más restrictivo.

2.6. Plan de Red de Alerta Temprana

Se trata de una red de comunicación con el fin que se establezca una red de alerta temprana de amenazas. Es un medio para difundir la situación de las amenazas aéreas para unidades sin sistemas de comando y control de defensa aérea y que sea comprendida adecuadamente. Estas redes alertan en el menor tiempo posible a todos los involucrados en las labores de seguridad.

2.7. Plan de Protección Priorizada (PPL)

Cada unidad se encarga de desarrollar un PPL (*Priorized Plan List*) para priorizar el uso de sus capacidades en función de la protección de sus activos. La criticidad asignada a los activos puede variar de acuerdo al objetivo y misión de cada unidad. Los activos pueden ser personas, propiedades, equipos, actividades en desarrollo, información, instalaciones, entre otros. A lo largo del desarrollo de operaciones de seguridad la priorización de activos puede variar de acuerdo al análisis del comandante y el concepto operacional determinado.

Desde la doctrina aérea, se puede adoptar la teoría de los 5 anillos y los Centros de Gravedad y que están asociados con la concentración de esfuerzos y centros de enfoque. Este modelo organiza los Centros de Gravedad por niveles alrededor de un centro. El primer nivel y centro del modelo es el liderazgo, sustentado por su importancia y capacidad de dirigir e influir en los demás niveles. En este nivel se pueden incluir los Centros de Comando y Control, Centro de Operaciones, Centros de Operaciones Tácticas, Centros de Operaciones de Brigada o el que aplique a cada institución. En el segundo nivel se encuentran los sistemas esenciales, que son comparables a los órganos vitales de un ser vivo como lo son los pulmones, el corazón, entre otros, que se asemejan a activos que brindan funciones y servicios indispensables como las comunicaciones. El tercer anillo hace referencia a la infraestructura, que hace referencia a toda aquella infraestructura físicas que permite cumplir sus funciones y objetivos. Encontramos en el cuarto nivel a la población, y dependiendo del ámbito en el que se aplique se identifica como todo el personal que sea susceptible a la agresión provocada por un enemigo. Finalmente, en el quinto nivel se encuentran las fuerzas armadas o activos de protección que actúan en función de la protección de la totalidad del sistema.

De acuerdo a lo anterior y al aplicar esta teoría al Plan de Protección Priorizada, la organización de prioridades es:

- Activos de liderazgo.
- Activos Esenciales.
- Infraestructura.
- Población/personal.
- Fuerza de seguridad.

Sin perjuicio de lo anterior, la Unidad organizará sus prelaciones conforme a sus prioridades y de acuerdo a su doctrina propia, misionalidad y objetivos.

INTENCIONALMENTE EN BLANCO

CAPÍTULO E. MEDIDAS Y EMPLEO C-UAS

1. Sinopsis

Una vez una amenaza UAS se encuentra en el aire, las unidades centran sus esfuerzos en mantener la supervivencia de la totalidad de sus activos. La supervivencia es la capacidad de evitar o resistir acciones hostiles y al mismo tiempo mantener la capacidad de cumplir su misión principal. A nivel táctico, diferentes factores contribuyen a aumentar los márgenes de supervivencia como los son la protección blindada, evitar la rutina, la movilidad y la conciencia situacional.

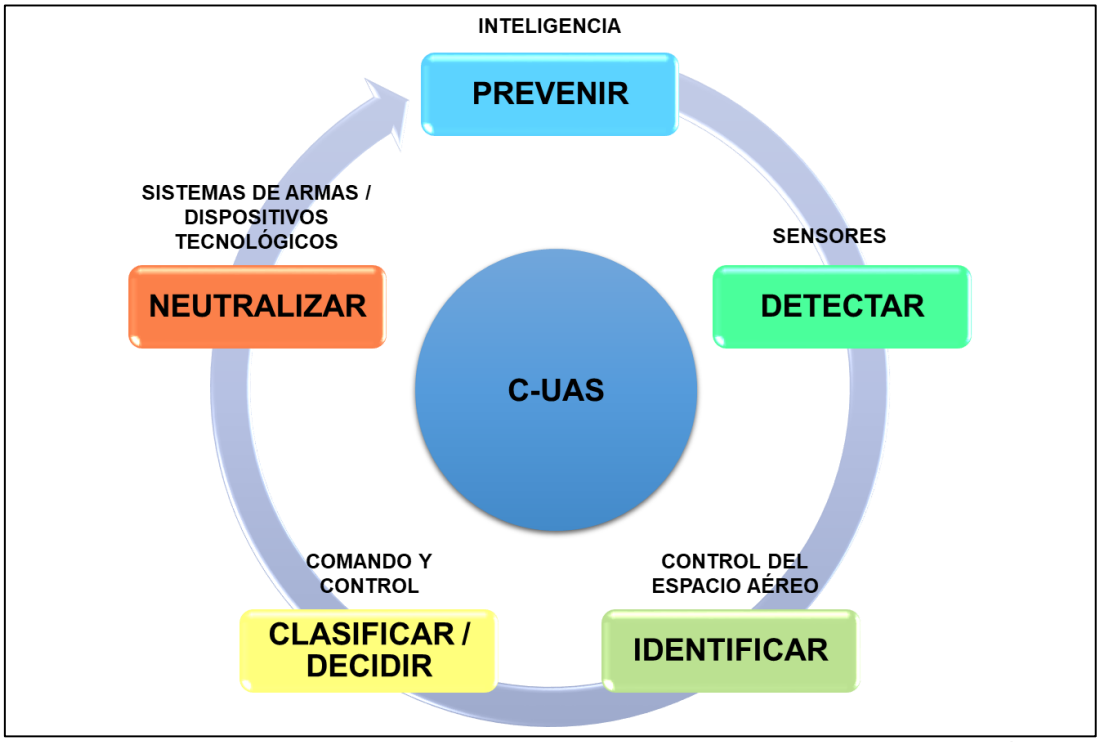
Teniendo en cuenta que el principal cometido de los UAS es la recopilación de información por medio de diferentes sensores, una vez sea detectada una amenaza UAS, se debe dar por supuesto que las unidades han sido observadas y analizadas. Aunque se cuente o no con sistemas C-UAS las unidades deben implementar medidas pasivas y activas para reducir la efectividad de los UAS hostiles.

A continuación, se presentan medidas y acciones defensivas pasivas y defensivas activas que los EAE podrán implementar para minimizar la afectación de la amenaza C-UAS.

Las medidas y acciones para el empleo de C-UAS están organizadas dentro de unas fases del Ciclo C-UAS. Las fases son: prevención como medida pasiva, detección, identificación, decisión y neutralización como medidas activas (Centro Conjunto de Desarrollo de Conceptos, 2019) como se muestra en la siguiente imagen:

INTENCIONALMENTE EN BLANCO

Ilustración 2: Diagrama Fases Ciclo C-UAS



Fuente: Construcción AAAES.

Para cada una de las fases, existen tecnologías y sensores disponibles en el mercado o en proceso de desarrollo. Sin embargo, al momento de definir cuál de estas se adapta más a las necesidades de cada área objeto de protección, deberán considerarse las ventajas y desventajas que presenta cada tipo de sensor, especialmente en lo relacionado a la posible interferencia que pueda generarse para las comunicaciones aeronáuticas y sistemas de ayudas para la navegación aérea.

Así mismo, durante los procesos de adquisición de UAS para la Fuerza Pública, es necesario identificar las vulnerabilidades propias de los sistemas frente al empleo de C-UAS y las medidas que deberán tomarse en el desarrollo de operaciones aéreas con el fin de mitigar los riesgos asociados.

2. Medidas Pasivas

2.1. Prevención

Dentro de las medidas pasivas se encuentran las medidas de prevención, las cuales contribuyen a la capacidad de supervivencia reduciendo la capacidad de detección y ataque a activos amigos y mitigar sus efectos potenciales. Las medidas pasivas y de prevención son la primera línea de defensa contra las amenazas aéreas. Aunque el principal objetivo de este documento es contrarrestar la amenaza C-UAS, estas

medidas son aplicables para cualquier operación antiaérea.

Algunas de las medidas son:

- Camuflaje y encubrimiento.
- Engaño
- Dispersión
- Desplazamiento
- Demarcación de áreas mediante señales informativas.

2.1.1. Camuflaje y encubrimiento

Entre más un objetivo se pueda confundir con su entorno, más difícil será su identificación desde el aire. Es el principio propio del camuflaje y para su óptimo empleo se debe considerar una alerta situacional alta sobre las condiciones del entorno.

Sin embargo, es importante tener en cuenta que los sensores a bordo de los UAS pueden operan en todo el espectro electromagnético. Por lo tanto, las labores de inteligencia y reconocimiento al enemigo facilitarían las labores de camuflaje y encubrimiento de los activos amigos. Por ejemplo, Si los datos de inteligencia indican que un UAV enemigo utiliza sensores visuales, entonces se emplean contramedidas visuales. Para sensores infrarrojos o radar, se emplean contramedidas que son efectivas en esos espectros.

A continuación, se presentan algunos conceptos que reducen la efectividad del empleo de sensores de diferentes espectros electromagnéticos.

- **Minimizar el movimiento.** El movimiento de vehículos, individuos o material puede llamar la atención del enemigo y generar condiciones que faciliten la detección por medio de sensores. Movimientos lentos, regulares o impredecibles, son algunas técnicas que se pueden aplicar para contrarrestar la amenaza.

INTENCIONALMENTE EN BLANCO

Ilustración 3: Vehículos en movimiento.

Fuente: "*New video shows Russian tank obliterated in strike*", CNN, 2023. (https://edition.cnn.com/videos/world/2024/01/23/ukraine-drone-strike-russian-oil-facility-tank-ebof-hnk-vpx.cnn).

En la ilustración 3, se puede apreciar cómo desde un sensor se revela la posición de vehículos ya que su movimiento genera estelas de polvo que son fácilmente detectadas por sensores en vuelo.

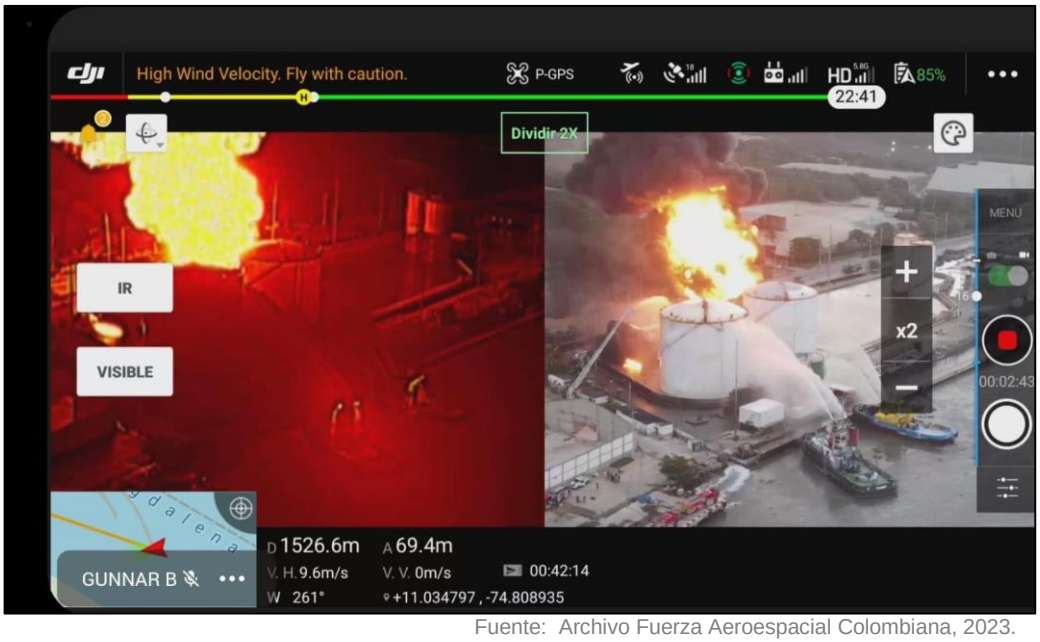
- **Evitar patrones predecibles**. El análisis y seguimiento que se pueda efectuar por parte del enemigo incrementa el impacto que pueda generar su actuar. Modificar las actividades rutinarias en las unidades amigas podría desestabilizar el análisis realizado por el enemigo-

- **Reflectancia**. La reflectancia es la cantidad energía (ondas electromagnéticas) que se reflejan en una superficie de un objeto. Dependiendo del espectro electromagnético se pueden presentar los siguientes tipos de reflectancia:

    - **Reflectancia Visual:** Dentro del espectro de ondas visuales, los colores pueden determinar la detección de un objeto. Asimismo, los contrastes de los colores permiten identificar formas de los objetos. La distancia de los sensores respecto a los objetivos puede variar la cantidad de contraste del objeto con su entorno y así, facilitar o dificultar la detección por medio de los sensores. Con condiciones de poca luz, la definición de los colores se hace más compleja.

    - **Reflectancia de temperatura**. La reluctancia de temperatura es la energía térmica reflejada por la superficie de los objetos. Dependiendo del nivel de reflectancia de temperatura, se generan contrastes térmicos que permiten la identificación de objetos. La luz del día puede afectar positiva o negativamente la información capturada por el sensor dependiendo de su uso, sin embargo, estos sensores son efectivos en condiciones nocturnas. Los objetos que generan su propia emisión de calor (motores, personas, plantas eléctricas), son altamente susceptibles a ser detectados por este tipo de sensores.

Ilustración 4: Comparación imágenes electroópticas e Infrarojas.



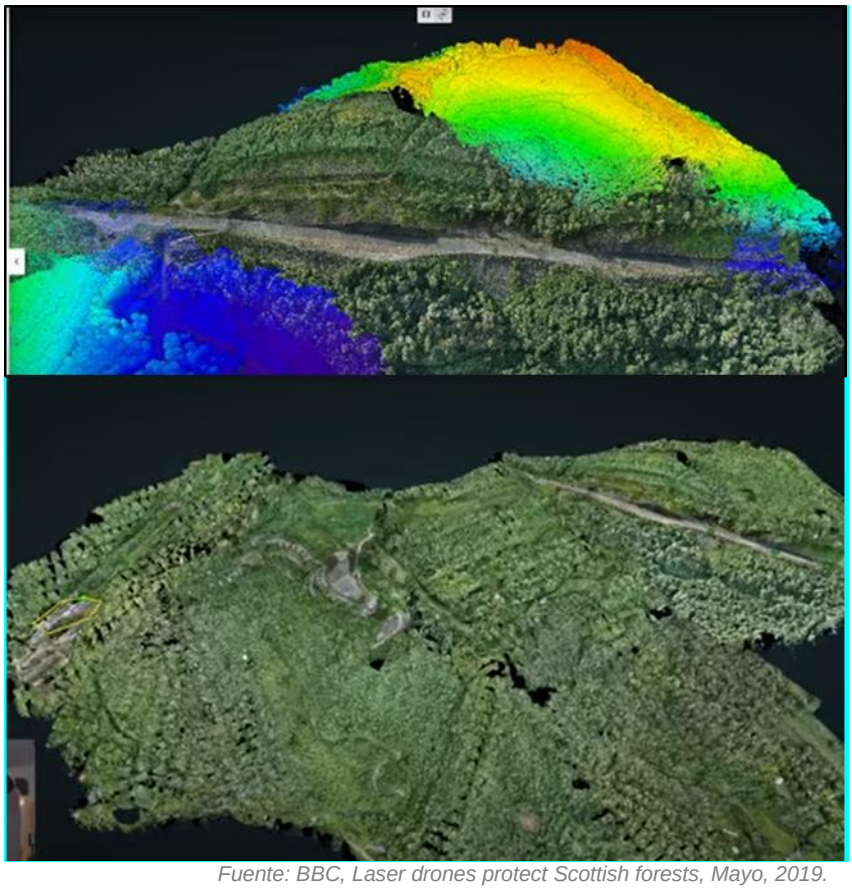
Fuente: Archivo Fuerza Aeroespacial Colombiana, 2023.

En la Ilustración 4, se puede observar la comparación de sensores Electroópticos e Infrarrojos. En este caso, se identifican las diferencias de los sensores a partir de emisiones de calor y energía generadas por una fuente de calor.

- **Reflectancia de señal radar.** Son ondas electromagnéticas de radiofrecuencia que se reflejan por efecto doppler en los objetos. Este tipo de reflectancia es comúnmente empleada para elaborar modelos 3D de objetos y se caracterizan por su alta precisión y definición.

INTENCIONALMENTE EN BLANCO

Ilustración 5: Modelo 3D a partir de sensores activos.



Fuente: BBC, Laser drones protect Scottish forests, Mayo, 2019. (https://www.bbc.com/news/uk-scotland-48380213).

La ilustración 5 contiene un modelo 3D generado a partir de sensores activos.

- **Forma**. Por medio de la forma de los objetos se puede facilitar la detección de objetivos. En la naturaleza, las formas de los objetos se caracterizan por ser irregulares. Sin embargo, objetos como vehículos o instalaciones se caracterizan por tener formas angulares, rectilíneas y bordes definidos que permiten la fácil identificación por medio de cualquier tipo de sensor. Distorsionar estas formas de los objetos puede dificultar su detección. El Ejército de los Estados Unidos emplea un tipo de malla ULCANS, que al cubrir objetos difumina sus formas y colores con su entorno. Este tipo de técnicas debe tener en cuenta el empleo operativo de algunos equipos por ejemplo en radares militares, podrían afectar su funcionamiento.

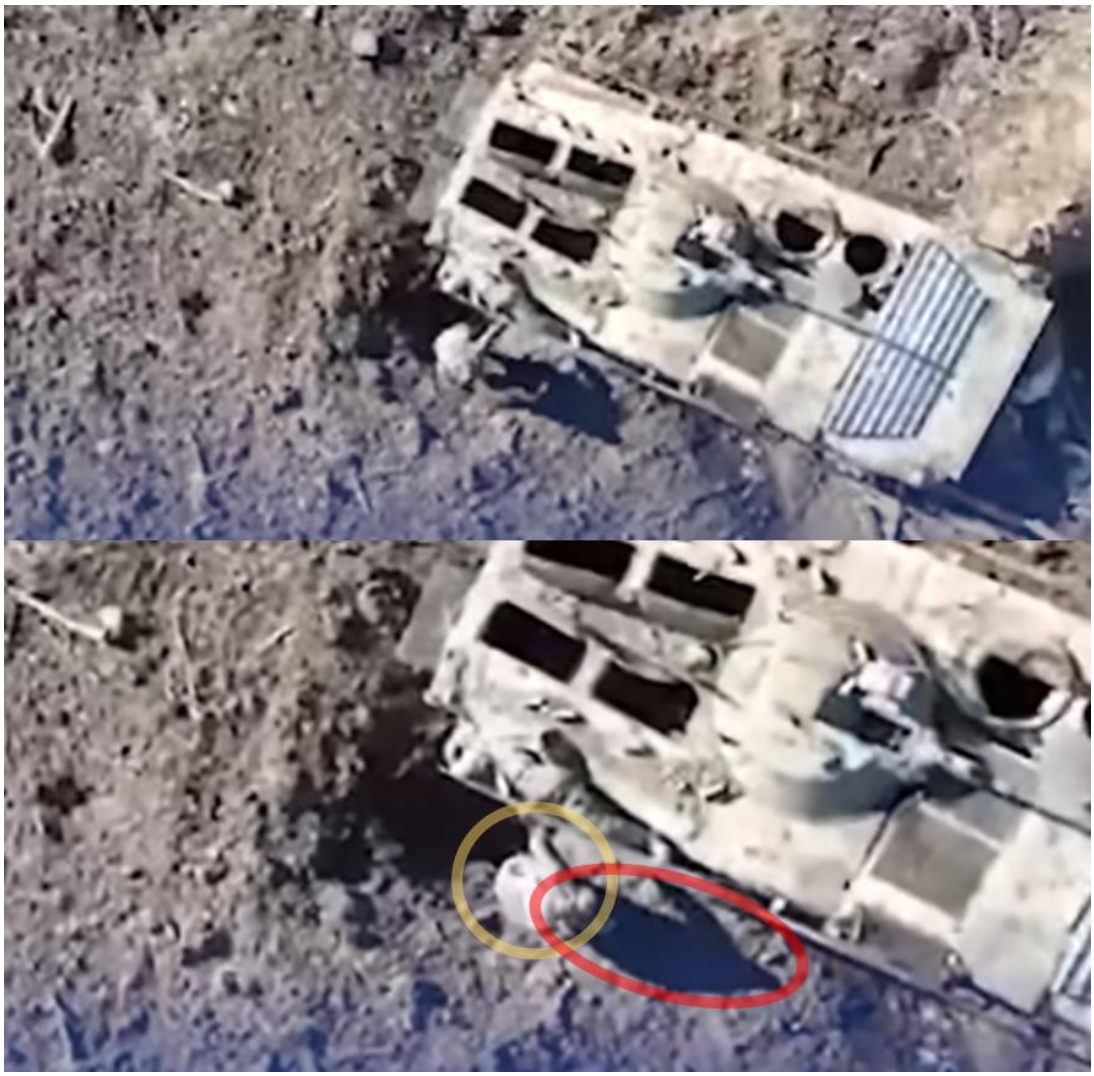
Ilustración 6: Detección de objetivos por medio de sensores.

Fuente: BBC, "*In Ukraine's river war, drones mean nowhere is safe*", enero 2024. (https://www.bbc.com/news/world-europe-67991772).

- **Sombras**. Por medio de las formas de las sombras se puede realizar la detección de un objeto desde el aire. Una sombra de un objeto proyectada en una superficie puede revelar información importante de ese objeto como su tamaño o disposición además de revelar su posición. Una sombra sobre una superficie puede incrementar el contraste de los objetos a su alrededor y facilitar su detección.

INTENCIONALMENTE EN BLANCO

Ilustración 7: Detección de objetivos por medio de proyección de sombras.



Fuente: CNN, “New video shows Russian tank obliterated in strike “(https://edition.cnn.com/videos/world/2024/01/23/ukraine-drone-strike-russian-oil-facility-tank-ebof-hnk-vpx.cnn).

En la Ilustración 7 se identifica que la sombra de un individuo permite revelar su posición debido a la proyección de la luz del sol respecto a su posición y a la posición del sensor. Pese a que su camuflaje es semejante a su entorno el contraste oscuro de la sombra se hace fácil para identificar.

- **Textura**. Desde el aire, una superficie rugosa parece más oscura que una superficie lisa, incluso si ambas superficies son del mismo color. Por ejemplo, las huellas de los vehículos cambian la textura del suelo dejando marcas claramente visibles. En superficies homogéneas como la nieve o arena del desierto las huellas de vehículos o de individuos son fácilmente detectables.

Ilustración 8: Caravana de vehículos detectados por UA.

Fuente: CNN, "*Ukraine's AI-enabled drones are trying to disrupt Russia's energy industry. So far, it's working*" abril 2024. (https://edition.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html).

Con la Ilustración 6 se puede observar que las huellas dejadas en el terreno por vehículos son fácilmente detectables por medio de los sensores de los UA.

2.1.2. Disciplina de camuflaje y encubrimiento

La disciplina de camuflaje y encubrimiento no es más que hacer un buen uso de las técnicas anteriormente descritas. Cualquier actividad por fuera de las actividades propias las unidades pueden deshacer los esfuerzos de las técnicas de camuflaje y ocultamiento.

Hace parte del camuflaje, la buena administración de luces, calor, ruido o desechos a todo nivel de la cadena de mando y puede significar la supervivencia de toda una unidad

Para misiones específicas, se pueden describir los procedimientos estándar relacionados con el camuflaje con tal de ser seguidos adecuadamente:

- Enumerar las responsabilidades específicas de contramedidas de camuflaje.
- Detallar los procedimientos para la conducta individual y de la unidad.
- Realizar ejercicios frecuentes con tal de identificar las mejores técnicas que permitan un camuflaje efectivo.

2.1.3. Fintas y engaño

Una de las técnicas es el empleo de señuelos que distraigan al enemigo. No se trata únicamente del empleo de réplicas o dummies, dependiendo de los sensores empleados por el enemigo, se pueden emplear firmas infrarrojas que confundan los

activos propios. Se pueden establecer ubicaciones falsas para desviar la atención de una actividad específica.

El uso adecuado de señuelos proporciona objetivos alternativos contra los cuales el enemigo gasta municiones, revelando posiblemente su posición en el proceso.

Ilustración 9: Helicóptero estacionado sobre aeronave pintada en el suelo.

Fuente: The Eurasian Times “Russian Chopper Lands On Su-30 Fighter Jet’s Silhouette”, Abril 2024. (https://www.eurasiantimes.com/russia-goofs-up-on-its-camouflage-paint-deception/#google_vignette)

La Ilustración 9 permite observar claramente un helicóptero estacionado sobre un aparente señuelo que simula una aeronave tipo SU-30 estacionado en una rampa militar. De esta manera, se evidencia la intención de tergiversar la información de inteligencia obtenida por sensores.

Los señuelos se utilizan para atraer la atención del enemigo con diversos fines tácticos. Su uso principal es desviar el fuego enemigo de activos críticos. Su diseño depende de varios factores, como el objetivo que se va a atraer, la situación táctica de una unidad, los recursos disponibles y el tiempo disponible para que una unidad se camufle y se oculte. Los señuelos son generalmente prescindibles y pueden ser elaborados o simples.

Los señuelos pueden ser empleados para forzar al enemigo a revelar su posición o sus capacidades.

El empleo adecuado de señuelos sirve para una serie de propósitos tácticos, que incluyen:

- Aumentar la capacidad de supervivencia del equipo y del personal.
- Engañar al enemigo sobre las capacidades, disposición e intenciones de las fuerzas amigas.
- Atraer el fuego enemigo, lo que revela sus posiciones.
- Alentar al enemigo a gastar municiones en objetivos de valor relativamente bajo (señuelos).

Hay tres factores altamente importantes para el empleo de señuelos:

- **Ubicación**. Una ubicación lógica de señuelos mejora enormemente su verosimilitud. Los señuelos suelen colocarse lo suficientemente cerca del objetivo real para convencer al enemigo de que ha encontrado el objetivo. Sin embargo, un señuelo debe estar lo suficientemente lejos para evitar daños colaterales al objetivo real cuando el señuelo atraiga fuego enemigo. El espacio adecuado entre un señuelo y un objetivo depende del tamaño del objetivo, los sensores de adquisición de objetivos enemigos esperados y el tipo de municiones dirigidas contra el objetivo.

- **Fidelidad (realismo).** Los señuelos se construyen de acuerdo con un procedimiento operativo estándar de unidad amiga e incluyen características del objetivo que un enemigo reconoce. Los señuelos más eficaces son aquellos que se parecen mucho al objetivo real tanto en términos de forma como de firmas electromagnéticas.

- **Replicar** completamente las firmas de algunos objetivos, particularmente objetivos grandes y complejos, puede resultar muy difícil. Por lo tanto, la construcción del señuelo debe abordar la región espectral electromagnética. Dentro de las técnicas se puede hacer más visible un objetivo señuelo que un objetivo real, con el fin de coaccionar al enemigo a enfocarse en el señuelo.

2.1.4. Dispersión

La dispersión es la esparcimiento o separación de tropas, material, establecimientos o actividades que generalmente se concentran en áreas limitadas para reducir la vulnerabilidad. Para aumentar su capacidad de supervivencia, las unidades

dispersan el personal y las capacidades en la mayor medida posible. La disipación de unidades y activos debe obedecer a las disposiciones del comandante de manera que se mantenga la comunicación entre las diferentes cadenas de mando y que se mantenga el apoyo mutuo.

Si bien existen diferentes variables que afectan el grado de dispersión de una unidad en un momento dado, el terreno suele ser un factor determinante clave en cuánto puede dispersarse una unidad. Generalmente, cuanto más abierto es el terreno, como lo son desiertos o tierras de cultivo, mayor es la capacidad de dispersión de una unidad para aumentar su capacidad de supervivencia contra amenazas aéreas.

2.1.5. Desplazamiento

Si se identifican activos amigos por parte del enemigo o comienza un ataque, las unidades pueden desplazarse a una ubicación alternativa para evitar ataques adicionales o hacer que el ataque actual sea ineficaz. Idealmente, un desplazamiento se realiza sin degradar el desempeño del objetivo principal de una unidad. Durante el proceso de planificación, la unidad tendrá en cuenta el empleo de UAS enemigos y sus capacidades conocidas.

3. Medidas Activas

Las medidas de defensa activas son una secuencia de varios pasos que las unidades y las cadenas de mando realizan para detectar, identificar, decidir y potencialmente enfrentarse a un UAS desconocido. Entre más rápido se puedan aplicar estos pasos, más eficaz será la respuesta contra las amenazas de UAS.

3.1. Detección

Los UAS son pequeños, maniobrables y silenciosos. Incluso para el ojo entrenado suelen ser muy difíciles de observar en vuelo. Las condiciones ambientales pueden hacer que dichos sistemas sean difíciles de detectar sin el uso de dispositivos tecnológicos especiales de seguimiento e identificación. La hora del día, los niveles de luz ambiental, las condiciones meteorológicas y el estado de alerta del observador afectarán la capacidad de observar un UAS potencialmente hostil. Además, un operador experimentado puede volar un UAS de manera táctica para mejorar aún más la capacidad de explotar las características del UAS. Esto puede incluir:

- Volar a bajo nivel, utilizando el terreno, obstáculos con extensión vertical y/o entorno urbano para enmascarar una aproximación a una posible ubicación objetivo.
- Uso de perfiles de vuelo dinámicos y erráticos para confundir y engañar al personal, lo que dificulta la observación visual.
- Usar el sol o las nubes para ocultar eficazmente el UAS de la vista.
- Uso de modos de vuelo deportivo para aumentar la velocidad y agilidad y minimizar

el tiempo de observación del UAS.

- Uso de múltiples UAS para confundir, engañar y abrumar a los observadores y dificultar el seguimiento.

Los tipos de sensores C-UAS y su ubicación determinan la capacidad de detección de las unidades. Los tipos de amenazas de UAS, el eje de avance de la amenaza, el terreno, el clima, el análisis de tiempo-distancia, los activos a ser defendidos, la zona de enfrentamiento deseada, los requisitos de vigilancia y la cantidad de activos disponibles son factores que afectan la mejor manera de colocar y emplear los sensores C-UAS.

El uso de varios tipos de sensores garantiza una detección más efectiva ya que actualmente no existe ningún tipo de sensor C-UAS que sea 100% efectivo.

En la medida de lo posible con el empleo de varios sensores C-UAS, el objetivo es formar una red de sensores integrada que incluya varios tipos de sensores. Las capacidades de sensores en apoyo de amenazas aéreas de bajo nivel deben planificarse en consecuencia su coordinación debe ser prevista. Los radares aeronáuticos son pueden ser empleados para ampliar la gama de sensores de detección.

Aunque se cuente con C-UAS, el personal involucrado en las funciones de seguridad debe ser consiente permanentemente de la amenaza aérea generada por los UAS.

3.1.1. Guardias aéreos

Los guardias aéreos deben estar atentos y con la vista puesta en el horizonte. Los guardias aéreos son responsables de detectar amenazas aéreas en las proximidades de la ubicación de la unidad y de brindar alerta temprana alertando a la unidad de posibles amenazas aéreas. Pueden estar equipados con el equipo óptico como binoculares para realizar técnicas de búsqueda y escaneo para reducir la capacidad del enemigo de evadir la detección.

Una técnica de detección visual de UAS es realizar un escaneo hasta 20° por encima del horizonte. Esto permitirá detectar vuelos demasiado bajos, pero identificar UAS que vuelen con una altura considerable. Cuando la ubicación de las unidades sea en elevaciones como montañas y riscos, el escaneo se puede realizar 20° por encima del horizonte y 20° por debajo del horizonte.
Alguna información que facilitará las labores de guardias aéreos son:

- Comprender las características de los posibles UAS que se consideran como amenaza.
- Comprender que los UAS se conforman de diferentes componentes para su funcionamiento como antenas, equipos de lanzamiento, entre otros.
- Comprender las condiciones actuales en el área relativas a los UAS enemigos.
- Estar equipados con elementos como binoculares, dispositivos de visión nocturna, miras térmicas y similares.
- Equipos C-UAS.
- Emplear fraseología adecuada y comunicación efectiva con los centros de

comando y control.
- Llamados de alerta estandarizados.
- Contar con mapas actualizados o grillas del área de responsabilidad.
- Emplear técnicas de orientación. (ubicación, rumbo, velocidad).

3.1.2. Alerta

Una vez se detecta una amenaza aérea, es necesario advertir rápidamente a todas las fuerzas amigas. Esto puede realizarse mediante dos métodos: un enfoque de arriba hacia debajo de la cadena de mando o un enfoque de abajo hacia arriba de la cadena de mando. Las aeronaves no tripuladas pequeñas suelen ser detectadas primero por las unidades avanzadas, por lo que es fundamental ensayar el uso de la red de alerta temprana de la unidad desde abajo hacia arriba de la cadena de mando. No importa qué enfoque se utilice, la información que se transmite se realiza empleando el formato de informe CAUCE-H. La recepción de este informe debería desencadenar acciones de seguimiento y alerta para los involucrados en funciones de seguridad. Cuando sea practicable, las unidades que detectan amenazas aéreas alertarán a las unidades adyacentes. La Tabla 4 muestra información adicional que se debe recopilar sobre la/s Aeronave/s No Tripulada/s desconocida/s mediante el formato CAUCE-H.

Tabla 4: *Formato CAUCE-H para recopilación de información.*

LINEA	INFORMACIÓN	EJEMPLO
1	Cantidad /Tamaño	Informar la cantidad de UA o tamaño de la formación.
2	Actividad	Reportar la actividad que posiblemente esté realizando: ¿Cuál es la dirección de movimiento? ¿Ha habido alguna acción hostil? ¿Está la UA sobre volando una única ubicación? ¿Está volando en línea recta? ¿A qué distancia probable se detectó la UA? ¿Se ha detectado un componente que haga parte de un UAS?
3	Ubicación	Reportar la ubicación de la actividad. Puede emplearse la grilla para reportar la ubicación.
4	Características	Incluye detalles como: Ala fija o multirotores Tamaño aproximado Número de motores o rotores Altura Si tiene sensores Características de las luces Cualquier característica que sea distinguible.
5	Equipamiento	Si se observa que transporte algún tipo de armamento u objeto relevante.
6	Hora	Hora en la que se detectó la actividad

3.1.3 Seguimiento

Simultáneamente con la alerta, las fuerzas amigas rastrean al objetivo y monitorean su movimiento. Es necesario realizar un seguimiento del objetivo hasta que se tome la decisión de neutralizar o no al objetivo. El plan de detección contribuye directamente a la capacidad de la unidad para rastrear objetos en el aire de forma continua y eficiente.

3.2. Identificación

La identificación es el proceso de determinar las características de un contacto desconocido detectado, principalmente si es hostil o si se trata de un UA que no se considera como amenaza. El empleo de capacidades C-UAS requiere una identificación temprana de los Sistemas de Aeronaves No Tripuladas para maximizar los tiempos de anticipación y evitar el fratricidio. Distinguir objetos aéreos amigos, neutrales u hostiles mientras se emplean sistemas de armas contra los UAS que se consideran como amenaza es una tarea muy compleja. El mismo tipo de UAS puede ser operado tanto por fuerzas amigas como enemigas. La identificación precisa permite a los comandantes tomar decisiones y mejorar la conciencia situacional. La identificación oportuna mejora las opciones de empleo de armas, ayuda a conservar los recursos amigos y reduce el riesgo de fuego amigo.

Existen dos métodos de identificación, positiva y procedimental. La identificación positiva es el método de operación más empleado. La identificación procedimental separa a los usuarios del espacio aéreo geográficamente, por altitud, rumbo, hora y maniobra. Para la realizar la identificación procedimental, se pueden hacer uso de los itinerarios de vuelo de aeronaves convencionales o de UAS en el área de interés para descartar que se trata de aeronaves amigas.

La identificación positiva es una identificación derivada de la observación y el análisis de las características del objetivo, incluido el reconocimiento visual, sistemas de soporte electrónico, técnicas de reconocimiento de objetivos individuales, u otras técnicas de identificación basadas en las características física y así, determinar si se trata de una detección hostil.

Por medio de la identificación positiva de un UAS se puede conducir a un nombre o categoría específica o a la marca y modelo exactos del UAS. Así mismo es de gran utilidad identificar su lugar de origen, sistemas de control u operador. La identificación de su carga útil también es importante si se puede determinar. Las características que ayudan a identificar un UA desconocido incluyen identificar:

- Si es de ala fija o de rotores.
- Estimado de su envergadura.
- Configuración de cola.
- Si es de un rotor/multirotor.
- Número de rotores.
- Altura.
- Tamaño estimado.
- Carga útil, tanto sensores como armas.

- Modelo, Marca
- Identificación de los componentes que hacen parte del UAS.

Durante la identificación los objetos detectados pueden categorizarse en:

- Objeto de interés. Es aquel que apenas ha sido identificado por los sistemas de detección y merece ser monitoreado para conocer sus intenciones y características.

- Objeto amigo. Es aquel que logró ser identificado, y por su características y comportamiento se deduce que está dentro del planeamiento del día para sobrevolar un sector determinado.

- Objeto Sospechoso. Es aquel que se considera inseguro ya que no se ha relacionado con las características o comportamiento de UAS propios o de fuerzas amigas.

- Objeto hostil. Es aquel objeto que por sus características y comportamiento se determina que es una amenaza para la seguridad de las unidades.

Ilustración 10: UA en vuelo con carga adherida a su estructura.

Fuente: CNN, "Ukraine's AI-enabled drones are trying to disrupt Russia's energy industry. So far, it's working" abril 2024. (https://edition.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html)

En la Ilustración 10, se aprecia un UA en vuelo en el que se puede observar que lleva adherida a su estructura una especie de carga. De acuerdo a la información de la fuente se trata de una carga explosiva empleada para neutralizar tanques y vehículos blindados en Ucrania.

3.3. Clasificar / Decidir

La fase de Clasificar / Decidir se divide en dos. En primer lugar, si existe la necesidad de enfrentar la amenaza. En segundo lugar, si se decide enfrentar la amenaza, se deciden los métodos a ser utilizados para disminuir o eliminar la amenaza previamente identificada por medio de la clasificación de los UAS y así prever los efectos de los métodos empleados para la neutralización. La clasificación puede apoyarse de la información recopilada durante el proceso de identificación.

Nota.- Puede emplearse la categorización dispuesta en el Capítulo B como herramienta para la clasificación del UAS.

Los métodos de neutralización pueden ser cinéticos y no cinéticos y algunas unidades podrán estar equipadas con capacidades cibernéticas o electromagnéticas. Cada eslabón de la cadena de mando debe ser consistente de las reglas de enfrentamiento (ROE), el espacio aéreo disponible, el potencial de daños colaterales y el derecho inherente de autodefensa.

Nota.- Dado a que la neutralización de los UAS puede resultar en daños a terceros, en el caso que ocurran, se deben informar las dependencias pertinentes para realizar los procedimientos respectivos de reparación.

Los métodos cinéticos atacan, destruyen o dañan el dispositivo para que no esté operativo.

Ejemplos de métodos cinéticos incluyen, entre otros:

- Municiones explosivas.
- Armas pequeñas.
- Proyectiles.
- Sistemas de Enredo.
    - Serpentinas.
    - Espuma en aerosol.
- Energía dirigida.
    - Láser.
    - Micro-ondas de alta potencia.
- Dispositivos de Captura.
    - Redes.

Los métodos no cinéticos para neutralizar dispositivos UA pueden ser interrumpiéndolo, bloqueándolo o controlando la señal entre el control de vuelo y de control terrestre del UA. Aunque se utilizan métodos no físicos en el UA, estos métodos aún pueden provocar que se estrelle y cause daños colaterales por lo que se debe tener en cuenta para la ejecución del procedimiento y despejar las áreas que podrían afectarse por estos efectos.

Ejemplos de métodos no cinéticos incluyen, entre otros:

- Interferencias de radiofrecuencia.
- GPS jamming.

- GPS.sproofing
- Dazzling.
- Interferencias de posición, navegación o sincronización (conocidas como PNT).

Algunos de los riesgos que se pueden presentar y deben evaluarse al iniciar la neutralización son:

- Riesgo de causar incidentes a unidades amigas, afectar a terceros u ocasionar daño colateral potencial.

- El incumplimiento de las ROE.

- Atacar objetivos sin tener la aprobación de la cadena de mando o sin seguir un plan de coordinación.

- Realizar ataques redundantes que desgasten los recursos limitados.

- Emplear sistemas C-UAS no óptimos o con efectos potenciales limitados.

3.4. Neutralizar

Las técnicas de neutralización comienzan una vez que ocurre la violación del espacio aéreo y se ordena por parte la autoridad competente atacar a los objetivos a nivel táctico.

La neutralización se ejecuta de acuerdo a las decisiones definidas en la fase de Decidir / Clasificar y las ROE.

Mientras se ejecuta el enfrentamiento, en lo posible, otros sistemas disponibles continúan haciendo seguimiento a el objeto detectado. Así, si el enfrentamiento no es efectivo, se puede realizar nuevamente como sea necesario.

Las medidas cinéticas o no cinéticas dan como resultado respuestas letales o no letales. En las respuestas no letales y una vez estas medidas sean empleadas es primordial asegurar que el enemigo no pueda operar el UA hasta que se realice un procedimiento de disposición del mismo. Dentro de las disposiciones a realizar, se contemplan los procedimientos a ejecutar si el UA transporta material explosivo o municiones.

En lo posible, se deben realizar esfuerzos para mantener íntegro el UA y si el UA se mantiene íntegro, una vez que esté asegurado, podrá someterse a análisis e inteligencia. Si la neutralización resultó en la destrucción del UA se deben hacer esfuerzos para recuperar los componentes para posterior análisis. Las acciones de análisis del UA son sumamente importantes debido a que el aparato o sus componentes pueden brindar información valiosa para mejorar las contramedidas empleadas por los EAE. Información de marca del aparato, seriales de fabricación, tarjetas o dispositivos de memoria, entre otros, pueden ser analizados para robustecer las medidas contra UAS.

Si el UA se mantiene íntegro, pero hay sospechas que contiene o transporta material explosivo, se deben realizar esfuerzos para neutralizarlo en áreas libres de afectaciones por explosivos y sus derivados. Una vez la situación esté controlada debe reportarse a personal capacitado quien dispondrá lo pertinente sobre éste material. Se debe determinar la zona de riesgo mientras se realizan las acciones de disposición explosivo y debe ser acordonada para minimizar el riesgo.

Si las acciones de neutralización no son efectivas, se debe continuar con los esfuerzos de seguimiento y si es necesario intentar las veces que sean necesarias las acciones de neutralización.

Finalmente, de las experiencias identificadas se deben replantear y reevaluar los procedimientos elaborados actuales como plan de mejora.

CAPÍTULO F. CONSIDERACIONES MÍNIMAS PARA LA ADQUISICIÓN E IMPLEMENTACIÓN DE C-UAS

Los EAE deberán tener en cuenta las siguientes consideraciones mínimas para la adquisición y empleo de C-UAS:

(a) El empleo de estos sistemas C-UAS generan un potencial riesgo, y por tanto los , EAE deberán propender por amparar el riesgo que dicho uso pueda generar por eventuales daños y perjuicios a terceros, de conformidad con lo dispuesto en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, y demás normas que regulen la materia de acuerdo a sus funciones, roles, misiones y capacidades distintivas.

(b) De acuerdo a los sistemas C-UAS a adquirir por los EAE, se deben elaborar los Conceptos de Operación (CONOPS) de Planeamiento de Empleo, Medidas y Empleo de los C-UAS. Los Conceptos de Operación deben ajustarse a su entorno, demás capacidades y misionalidad.

Los Conceptos de Operación, son documentos en los que se incluyen requerimientos de alto nivel que proporcionan un mecanismo para que los usuarios describan sus expectativas del sistema. El objetivo de los CONOPS es enfocar los procesos en un análisis conceptual.

Algunas de las características de los CONOPS son:

- Describe un sistema supuesto o ideal.
- Es aplicable a distintos tipos de usuarios.
- Identifica diferentes modos de operación.
- Esclarece posibles necesidades de los usuarios.
- Prioriza las necesidades deseadas de los usuarios.
- Apoya el proceso de toma de decisiones
- Contempla una variedad amplia de amenazas y cursos de acción. Su aplicación depende del entorno operacional.

(c) Un factor clave para determinar la viabilidad de instalar un sistema de detección o alrededor de un área objetivo (Unidad Militar y/o policial, aeropuerto, edificio, entre otros) es la cantidad de sensores necesarios para lograr la cobertura deseada del espacio aéreo. Debido a que el volumen de cobertura depende de las características y requisitos únicos de cada objetivo y del tipo de sistema, la cantidad de sensores variará. La distancia de cobertura para muchos tipos de tecnologías de detección también limita la eficacia de dichos sistemas para determinar las ubicaciones de los UAS y su punto de control. Además, es posible que las áreas de cobertura necesiten abarcar ángulos más amplios, ya que, el Piloto Remoto y/u Operador pueden no estar cerca del UAS.

(d) No existe una única solución tecnológica C-UAS LSS que sea efectiva contra toda amenaza, en todo momento y lugar, por lo que se debe considerar qué tipo de sistema es más adecuado para cada escenario de empleo del EAE, entorno y

situación general del objetivo a proteger. En este sentido, se debe evaluar no solo la protección de los activos estratégicos y la infraestructura critica de la nación, sino también de las unidades e instalaciones militares y de policía dentro del territorio nacional, entre las que destacan principalmente las bases aéreas y aeródromos de operación de la Fuerza Pública e incluso la áreas donde normalmente operan helicópteros de los EAE por su complejidad y el impacto en la seguridad operacional que podría llegar a tener el empleo incorrecto de UAS LSS sobre las operaciones aérea que en ellas se desarrolla.

(e) Así mismo, la protección de los buques y demás Unidades a flote de la Armada Nacional de Colombia, tanto anclados y durante las entradas y salidas de puerto, como durante las navegaciones, requerirá de sistemas C-UAS LSS adecuados a dichas situaciones.

(f) Los sistemas C-UAS LSS deberán ser modulares, escalables, rápidamente actualizables para adaptarse a la evolución de la amenaza; que permitan la integración de diferentes tipos de sensores para la detección, identificación, decisión, y de sistemas para la neutralización; que se basen en la cooperación de tecnologías complementarias (radar, optrónica, acústica, energía dirigida, submuniciones, entre otros); que tengan fácil movilidad, portabilidad y que cumpla con los requerimientos mínimos para su puesta en funcionamiento tras un cambio de ubicación (Centro Conjunto de Desarrollo de Conceptos, 2019).

(g) Los sistemas C-UAS LSS más complejos deberán disponer de un alto grado de automatización, que permita un proceso de decisión ágil. Debido al escaso tiempo de respuesta del que disponen los sistemas C-UAS LSS, las fases de detección, identificación y la recomendación de decisión (neutralizar o no) deberían realizarse de forma automática. La fase de neutralización se debería poder configurar en modos de operación manual, semiautomático y automático, dependiendo de la amenaza, escenario, entorno, situación, estado de alerta y reglas de enfrentamiento vigentes. Así mismo, las interfaces de los sistemas deben poder ser integradas desde centros de monitoreo y así mismo poder interactuar con los demás sistemas electrónicos de seguridad disponibles. (Centro Conjunto de Desarrollo de Conceptos, 2019).

(h) Si bien los sistemas C-UAS LSS podrían llegar a tener la capacidad de interconectarse e integrarse mediante un sistema de C2 con el resto de los sistemas de Defensa Aérea (DA) y de Protección a Fuerza (PF), se considera que en el corto y medio plazo la integración debería ser como mínimo a nivel local de cada sistema C-UAS LSS, para asegurar un ciclo de decisión del operador adecuado en cuanto a la neutralización o no del UAS LSS detectado. Hasta que la tecnología no permita una integración completa de los sistemas C-UAS LSS en el Sistema de Defensa Aérea, ésta se llevará a cabo mediante procedimientos y comunicaciones directas.

(i) Se deberá buscar la sencillez en la operación y el mantenimiento, con el fin de que su empleo solo requiera un determinado nivel de especialización y no de especificidad, reducir las necesidades de Instrucción y Adiestramiento (I+A) y la huella logística para el despliegue.

(j) Los sistemas C-UAS LSS deberán tener un alto grado de disponibilidad operativa,

que les permita su funcionamiento en ciclos de 24/7, lo que requerirá de sistemas con una alta fiabilidad y mantenimientos programados que se puedan ejecutar con rapidez.

(k) La capacidad C-UAS LSS debe ir más allá de los sensores y sistemas necesarios para la detección, identificación y neutralización de los UAS LSS. Se considera necesario actuar contra el adversario que ha decidido emplearlos de forma hostil contra el EAE. Para ello, la explotación técnica de la información obtenida de los componentes y capacidades de los UAS LSS neutralizados, apoyaría la fase de prevención del ciclo C-UAS LSS. De la misma forma es vital que los EAE generen y compartan con sus estamentos de inteligencia datos estadísticos de las detecciones de UAS hostiles a la AE y/u organismos civiles. Esto servirá como un insumo para que los organismos de inteligencia institucionales y nacionales realicen búsquedas de información puntuales que fortalezcan los productos que generan estas agencias.

(l) Las necesidades de infraestructura vendrán condicionadas por el tipo de sistema C-UAS LSS (portátil/fijo/móvil), los diferentes sistemas que lo compongan (sensores de detección e identificación, sistema C2, sistema de neutralización) y el nivel de integración que se determine (aislado, local, C2, total). Se considera que el mantenimiento de los sistemas C-UAS LSS se podría realizar en las infraestructuras actuales. No obstante, se debería procurar que las necesidades de instalación sean las mínimas posibles y limitadas al emplazamiento físico del sistema.

(m) La nueva capacidad C-UAS LSS implicará que los EAE revisen y adapten la doctrina existente conjunta, específica y combinada, sobre la utilización de las diferentes capacidades afectadas por la misma, así como analizar la posibilidad de creación de una doctrina particular. La evolución será muy rápida, por lo que se debería desarrollar en paralelo a los nuevos sistemas, para que la solución al problema no pierda eficacia o se quede obsoleta en un corto periodo de tiempo.

(n) El Anexo 2 de esta guía “Consideraciones Técnicas para la selección de C-UAS”, provee una orientación con preguntas que pueden ser empleadas por los EAE, dentro de los procesos de elección de Sistemas C-UAS, con el fin de orientar adecuadamente la información que requiere el EAE por parte de las empresas fabricantes para tomar decisiones adecuadas en la adquisición de este tipo de equipos, propendiendo por una estandarización tecnológica que favorezca la escalabilidad de los equipos, el desarrollo y línea logística asociada a estos equipos.

Autores:

Goliath
Jefe Oficina Autoridad Aeronáutica Aviación de Estado

Fencer
Especialista Estratégico Autoridad Aeronáutica Aviación de Estado

ANEXO 1
CARACTERÍSTICAS Y LIMITACIONES DE SISTEMAS C-UAS DE MAYOR EMPLEO

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
Láser Ejemplos: Boeing YAL-1 / ABL (Airbone Laser) AN/SEQ-3 Laser Weapon System (XN-1 LaWS) MEHEL Rheinmetall HEL	Un láser es un dispositivo que produce un haz intenso y unidireccional de luz coherente. A diferencia de la luz ordinaria, generada por el sol o una bombilla, el rayo láser es coherente y casi uniforme en longitud de onda, y viaja en una sola dirección. Hay dos formas por las cuales un láser puede destruir un objetivo: destrucción térmica y destrucción mecánica. La destrucción térmica se produce cuando la energía térmica dirigida por un arma láser permanece en el mismo punto en un objetivo, es absorbida por la superficie objetivo y, por lo tanto, da como resultado el calentamiento por el efecto Joule. Con suficiente precisión y tiempo de permanencia, tras la fusión empezará a vaporizarse. La destrucción mecánica o «destrucción por impulso» ocurre cuando los pulsos de láser cortos e intensos interactúan con la superficie del objetivo, creando una onda de choque que penetra en el objetivo, pudiendo causar un colapso estructural y destruir componentes mecánicos internos.	Reducción drástica de los costes tanto de adquisición, como de operación y empleo.	El haz láser en su desplazamiento se ve afectado por las partículas presentes en la atmosfera como vapor de agua, dióxido de carbono, humo o calima.
		Concepto de sistemas de armas con mantenimiento y piezas de repuesto reducido.	Existen materiales resistentes a la acción del láser, por lo que podría ser inefectivo frente amenazas revestidas de materiales que reflejen la energía láser.
		Al ser un arma electromagnética el desplazamiento del rayo láser se produce a la velocidad de la luz, por lo que su efecto es casi instantáneo.	A diferencia de gran multitud de sistemas de armas cinéticos, necesita mantener constantemente la línea de visión sobre el objetivo.
		A diferencia de un sistema de armas cinético, el número de disparos disponible únicamente dependerá de la capacidad del sistema de armas de suministrar corriente eléctrica y de la refrigeración del mismo.	No puede iluminar a varios objetivos a la vez, por lo que en caso de multiamenaza son necesarios varios sistemas láser o complementarlo con otros sistemas de armas.
		Flexibles y modulares.	La potencia alcanzada hasta ahora en los sistemas de armas láser es insuficiente para amenazas aéreas no tripuladas de Clase II o superior.
		Pueden operar a cualquier nivel de potencia hasta su máximo nominal, por lo que permite al operador adaptar el efecto deseado en función de la situación táctica.	

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
Sistemas de armas de microondas de alta potencia (HPM) Ejemplos: RANETS-E PHASER HPEM counter UAS Counter-electronics High Powered Advanced Missile Project (CHAMP)	Son otro tipo de arma de energía dirigida, que tiene una longitud de onda mucho más larga y una frecuencia mucho más baja que el láser. Las armas HPM generalmente se subcategorizan como sistemas de banda estrecha (NB) o banda ultra ancha (UWB). Los sistemas de HPM de banda estrecha tienen mejores características de transmisión y menos problemas con el fratricidio que los sistemas de banda ultra ancha. Además, los sistemas de banda estrecha requieren un conocimiento previo de la amenaza para identificar la frecuencia específica de interés y son más susceptibles a contramedidas. Las armas HPM de banda ultra ancha proporcionan un amplio rango de capacidades incluso con poco o ningún conocimiento del objetivo. Dado que la destructividad de las armas HPM de banda ultra ancha depende de su distancia al objetivo, tienen un alcance efectivo más corto que las armas de banda estrecha que generalmente tienen una mayor potencia radiada. La energía de HPM puede afectar a cualquier cosa que responda a tensiones y corrientes inducidas electromagnéticamente.	Al igual que las armas láser, son una opción económica en comparación con los sistemas de armas cinéticos.	El alcance de las armas HPM es muy discreto en comparación con muchos sistemas de armas cinéticos. Este depende de la frecuencia generada, la distancia al objetivo y la susceptibilidad del objetivo
		Como arma electromagnética su acción es casi instantánea. A diferencia del láser no le afectan las condiciones atmosféricas para su operación.	Existen multitud de posibilidades para proteger un sistema frente al ataque por HPM. Instalación de cajas de Faraday, filtros, conductores de fibra óptica, antenas específicas o uso de láminas conductoras sobre uniones.
		A diferencia de los láseres, las armas HPM pueden atacar a múltiples objetivos y para que sean efectivas no necesitan tanta precisión como un láser. Es por ello por lo que son muy efectivas frente a enjambres de UAS.	A diferencia del láser, el riesgo de fratricidio con armas HPM es elevado. Cualquier cosa susceptible al HPM en su rango de cobertura será afectada. Son necesarios procedimientos o conos de cobertura en los que no operen fuerzas amigas, así como medidas de protección propias frente a este tipo de armas.
		Permiten diferentes efectos sobre los objetivos dependiendo de la potencia de emisión. Incluso pueden producir daños en equipos apagados.	Emiten una firma electrónica fácilmente localizable, por lo que pueden delatar la posición al enemigo y ser objeto de ataque por parte de este.

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
Interferencia electromagnética (*Electromagnetic Jamming*) Ejemplos: J4SKY-T Virtual-Fence AUDS Anti-UAV Defence System R-330ZH DroneGun	La interferencia puede ser vista como una señal no deseada dentro del rango de operación de un determinado sistema de comunicación. La calidad de un sistema de telecomunicación está directamente ligada a la relación entre la potencia de señal deseada y la potencia de ruido más la interferencia (SINR - *Signal to Interference plus Noise Ratio*) captada por el receptor dentro de la banda de transmisión. De esta manera, cualquiera que sea el tipo de interferencia, se tendrá una reducción de esa relación y, consecuentemente, una degradación en la calidad de la comunicación. Las interferencias intencionales son aquellas generadas de forma deliberada, a fin de inviabilizar el establecimiento de enlaces de comunicación en determinadas frecuencias. El jamming es la radiación deliberada, reradiación o reflejo de la energía electromagnética con el fin de prevenir o reducir el uso efectivo del espectro electromagnético por parte del enemigo, con la intención de degradar o neutralizar la capacidad de combate del miso. Su efectividad dependerá de la técnica usada y de las características del objetivo. Los UAS LSS, generalmente, si son controlados a distancia están transmitiendo señales de RF, bien sean de control, de video o de posición. Por otro lado, si siguen una ruta de vuelo preprogramada, en la que vuelan de forma autónoma, utilizan señales de alguno de los sistemas globales de navegación por satélite para seguir la misma.	**Jamming link de datos**	**Jamming link de datos**
		Como arma electromagnética su acción es casi instantánea. Además, son sistemas muy económicos y efectivos frente a amenazas no protegidas.	Las bandas de RF en las que operan son utilizadas por sistemas de telefonía móvil, telecomunicaciones o redes Wi-Fi entre otros, por lo que su acción puede afectar a sistemas propios o sistemas no deseados.
		Hay disponibles sistemas de *jamming* tanto direccionales para una amenaza localizada, como omnidireccionales para cubrir grandes áreas.	En diversos países hay bandas de frecuencia que están protegidas, por lo que su interferencia solo puede ser autorizada por el Gobierno.
		Permiten una acción dirigida pudiendo atacar el enlace de datos de video, telemetría y control.	Actualmente existen multitud de desarrollos tecnológicos tanto civiles como militares para evitar las interferencias en su sistema de comunicación.
		Generalmente neutralizan la amenaza sin destruirla. En este sentido puede permitir capturar el UAS enemigo (por ejemplo, si la aeronave entra en modo pérdida de link y efectúa aterrizaje de emergencia) o incluso localizar al operador en el caso de UAS LSS (por ejemplo, persiguiendo a un dron en situación de *Regreso a casa*).	Dado un caso de *jamming* sobre una amenaza por UAS LSS en el que esta revierte a modo seguro de retorno a punto de origen, si el atacante selecciona como punto de origen las coordenadas del objetivo deseado se daría la situación en la que el *jamming* del sistema de armas aproxime la amenaza al objetivo.
		Son altamente flexibles pudiéndose instalar en localizaciones fijas o móviles.	Gran número de UAS pueden ser programados para operar autónomamente sin la necesidad de un link de datos con el operador, por lo que los sistemas de armas *jamming* en este caso serían totalmente inefectivos.
		Jamming señal GNSS	**Jamming señal GNSS**
		Sistemas muy económicos y tecnológicamente sencillos.	Su empleo con sistemas omnidireccionales puede afectar a sistemas propios o no deseados.
		Altamente efectivos para UAS que operan de manera autónoma, inhabilitando su guía u obligando al operador a tomar el control. Para UAS de ala fija la información de los sistemas GNSS es vital en la maniobra de aterrizaje (un error del sistema de navegación de 1 metro se traduce en una imprecisión de 10 metros en el punto de aterrizaje).	Actualmente existe multitud de sistemas de navegación dual GNSS/inercial, de tal manera que si el UAS pierde la señal satélite pasa a navegación autónoma con sistema inercial. El sistema inercial es menos preciso que el satelital, pero puede ser suficiente en el caso de UAS hostiles atacando objetivos de dimensiones moderadas.
		Para el caso de los UAS LSS, una pérdida de señal válida de un sistema GNSS puede provocar la colisión contra el terreno o contra objetos colindantes.	Existen antenas con tecnología anti-*jamming* de GNSS. Por otro lado, hay numerosos programas que están desarrollando soluciones tecnológicas para evitar el *jamming* GNSS.
		Pueden ser direccionales u omnidireccionales, cubriendo grandes áreas.	La acción del *jamming* de la señal GNSS sobre un UAS controlado por un operador puede no ser suficiente para neutralizarlo.
		Altamente efectivos frente a enjambres de UAS.	
		Son altamente flexibles, pudiéndose instalar en sitios fijos o móviles.	

TIPO DE SISTEMA	CARACTERÍSTICAS	CAPACIDADES	DEBILIDADES
Spoofing	Es un tipo de ataque a la lógica de las aplicaciones. El tipo más común frente a drones es el *spoofing* de la señal GNSS. Consiste en la transmisión deliberada de una señal falsa de GNSS con la intención de engañar a un receptor proporcionándole información falsa de posición, velocidad y tiempo. El objetivo del ataque spoofing es forzar de manera inadvertida al receptor GNSS a seguir la señal modificada con el objetivo de inducir un error de posición. Realizar spoofing sobre las bandas encriptadas de los sistemas GNSS como la banda P (Y) de GPS o la banda PRS del Galileo es prácticamente imposible. Sin embargo, en estos casos un tipo de ataque efectivo es el Meaconing, que consiste en grabar señales encriptadas y re-radiarlas posteriormente. Si el receptor interpreta estas señales como válidas, estará asumiendo un error.	Proveen un tipo de ataque muy económico y tecnológicamente sencillo.	Su empleo con sistemas omnidireccionales puede afectar a sistemas propios o no deseados.
		Altamente efectivos para drones que operan de manera autónoma con sistema GNSS no encriptado.	Necesita de operadores con conocimientos avanzados a diferencia de otros sistemas de armas no cinéticos.
		Accesibles tanto en el mercado civil como el militar.	Frente a señales GNSS encriptadas sus efectos son limitados. Para estos casos se puede emplear *Meaconing*.
		Pueden permitir el control y captura de un UAS o su destrucción, guiando al mismo a un área de control o haciéndole volar a un lugar donde colisione.	Existen numerosos desarrollos tecnológicos para detectar ataques *spoofing*.
		Pueden pasar inadvertidos para el enemigo, de tal manera que no sepa que sus UAS estén siendo atacados con sistemas de *spoofing*.	La acción del *spoofing* de la señal GNSS sobre un UAS controlado por un operador puede no ser suficiente para neutralizarlo.
			En el caso de un ataque por enjambre y una sola antena para *spoofing* disponible, la señal enviada será similar para todas las aeronaves del enjambre independientemente de su posición, por lo que es necesario un estudio situacional para evitar que alguno de los UAS se dirija al lugar a proteger.
			Su alcance es limitado.
Hacking *Ejemplo: Maldrone*	Tanto UAS como estaciones en tierra (GCS) son susceptibles a ciberataques en sus diferentes segmentos o subsistemas. Entre los ataques más comunes destacan la exposición a virus informáticos de las GCS, ataque sobre el link de comunicaciones entre aeronave y GCS o ataque al sistema operativo propio del UAS.	Son un tipo de ataque muy económico.	Necesita de operadores altamente especializados y con amplios conocimientos de la plataforma a atacar.
		Altamente efectivos para UAS no protegidos frente a ciberataques.	Ante UAS protegidos frente a ciberataques su acción puede ser extremadamente compleja.
		Pueden permitir el acceso a información de sensores, control o destrucción del UAS.	Existen numerosos desarrollos tecnológicos para protegerse frente a ciberataques, como sistemas de comunicaciones encriptadas, cortafuegos...
		Pueden pasar inadvertidos para el enemigo.	

Fuente: Instituto Español de Estudios Estratégicos. (2018). *El sistema de defensa aérea no cinético, clave para la defensa anti drone.* Madrid.

ANEXO 2
CONSIDERACIONES TÉCNICAS PARA LA SELECCIÓN DE C-UAS

En referencia al documento "*Unmanned Aircraft System Detection-Technical Considerations*" de la FAA, se consolidan en esta guía una serie de preguntas que pueden ser empleadas por los EAE durante los procesos de estructuración de procesos cuyo fin sea el de optar por la adquisición de equipos C-UAS para la protección de Unidades Militares y/o Policiales, especialmente cuando estas cuentan con aeródromos como parte integral de su infraestructura.

En referencia al contenido de la Guía, su contenido es un criterio orientador que permite vislumbrar una operación óptima de acuerdo a requerimientos específicos y condiciones individuales de diferentes posibles escenarios operacionales que se complementa con el contenido expuesto a continuación para lograr la adquisición de sistemas adecuados, eficientes y, sobretodo, acordes a los requerimientos propios de cada EAE.

PARTE 1: MITIGACIÓN

La mitigación o contramedidas de UAS incluyen la capacidad de interrumpir, deshabilitar, destruir, tomar el control y/o proporcionar instrucciones de vuelo alternativas a un UAS objetivo. Algunos sistemas de detección de UAS pueden tener estas capacidades integradas, con la posibilidad de ser desactivadas, mientras que otros pueden ofrecerlas como una capacidad modular opcional.

Pregunta	*Información Adicional*
¿En las unidades se aplican medidas de disuasión o de reducción de efectividad de los UAS?	
¿Hay actividades o activos que deban priorizarse para ser protegidos por los C-UAS?	
¿El sistema de mitigación UAS tiene alguna capacidad para realizar actividades de contramedida?	Si es así, ¿cómo se desactiva?
¿Qué tecnologías o métodos de contramedidas emplea el sistema?	Ej: Cinético, Cinética híbrida, no cinética, RF, Jamming, Laser, entre otros.
¿Qué tipo de interferencia o afectación se puede generar a las comunicaciones aeronáuticas o frecuencias usadas por los sistemas de navegación en tierra y/o a bordo de las aeronaves cuando se activan las contramedidas?	
¿Qué frecuencias se emplean para la operación de las contramedidas?	
¿Se tiene conocimiento o se han evidenciado consecuencias no esperadas y/o planeadas al activar las contramedidas durante el tiempo en que han sido implementadas?	

PARTE 2: DETECCIÓN PRIMARIA (RF Y RADAR)

Un factor clave para determinar la viabilidad de instalar un sistema de detección en o alrededor de un área objetivo (unidad militar o policial, aeropuerto, edificio, entre otros) es la cantidad de sensores necesarios para lograr la cobertura deseada del espacio aéreo. Debido a que el volumen de cobertura depende de las características y requisitos únicos de cada objetivo y del tipo de sistema, la cantidad de sensores variará. La distancia de cobertura para muchos tipos de tecnologías de detección también limita la eficacia de dichos sistemas para determinar las ubicaciones de los UAS y su punto de control. Además, es posible que las áreas de cobertura necesiten abarcar ángulos más amplios, ya que, el piloto al mando y/u operador pueden no estar cerca del UAS.

Así mismo, los fabricantes o vendedores pueden identificar los sistemas que empelan RF como no emisores (a menudo usando el término "pasivo") aunque el producto podría incluir y emplear regularmente tales capacidades de emisión, que podrían interferir con otras facilidades necesarias para la operación aérea.

Pregunta	*Información Adicional*
¿Cuáles son las áreas de cobertura, las ubicaciones críticas del sitio y los volúmenes de espacio aéreo que se deben monitorear?	
¿Se cuenta con los contactos apropiados de control de tránsito aéreo o de Defensa Aérea que permita conocer o descartar trazas de interés?	
¿Cuáles son las tecnologías o sensores utilizados como medio principal para la detección?	Ej: Radar, RF, EO / IR, acústicos, entre otros.
¿Cuáles son las tecnologías o sensores utilizados como medios secundarios o de apoyo para validar la actividad detectada por los sensores primarios?	Ej: Radar, RF, EO / IR, acústicos, entre otros.
¿Se ha realizado un análisis de RF para este sitio específico?	¿Quién realizó el análisis? ¿Las emisiones de RF fueron simuladas o reales?
¿Cuál es el área de cobertura por sensor o del Radar?	¿Azimut? ¿Altitud? ¿Distancia?
¿Cuántos de cada tipo de sensor se requieren para el área requerida para el área objetivo?	
¿Cuáles son las capacidades de filtrado que utiliza el sistema para reducir la RF de fondo y la interferencia con otros sistemas?	
¿El sistema de detección depende de una base de datos de firmas de RF o radar conocidas?	En caso afirmativo, ¿con qué frecuencia se actualiza la base de datos? ¿Cuál es el proceso para actualizar la base de

	datos? ¿Hay un costo continuo para las actualizaciones de la base de datos?
¿El sistema puede detectar una operación de UAS o quién está saltando o cambiando intencionalmente las frecuencias a una velocidad aleatoria y / o rápida para evadir la detección?	
¿El sistema intercepta la transmisión de video en vivo de la UAS?	
¿El sistema diferencia y rastrea múltiples objetivos simultáneamente?	Si es así, ¿cuál es el límite superior en el número de objetivos que puede rastrear?
¿Se han realizado evaluaciones de la propagación de RF durante el día y la noche para tener en cuenta cualquier posible interferencia electromagnética que pudiera generarse?	
¿Cuál es la potencia de transmisión del radar?	
¿Cuáles son las bandas de frecuencia del radar?	¿Cuál es el tipo de escaneo del radar?
¿Cómo afectan las condiciones meteorológicas al radar?	

Es importante considerar, además, que ciertos modos de vuelo de la aeronave (por ejemplo, el vuelo estacionario) y el grado de autonomía de vuelo pueden limitar la efectividad del sistema de detección.

Pregunta	*Información Adicional*
¿Qué tipos de UAS puede detectar el sistema? RF y RADAR	Ej: Ala fija, multirotor, entre otros.
¿Cuánto tiempo tarda el sistema en detectar un UAS que está dentro del alcance? RF y RADAR	Ej: Cinético, Cinética híbrida, no cinética, RF, Jamming, Laser, entre otros.

Así mismo, es probable que se necesite mano de obra dedicada y capacitación especializada para operar el equipo y ayudar a discernir falsos positivos, teniendo en cuenta que el sistema de detección puede identificar incorrectamente otro objeto en movimiento como un UAS.

Pregunta	*Información Adicional*
¿Cómo diferencia el sistema entre la detección de un posible elemento de interés y un UAS?	
¿El sistema detecta UAS semiautónomos (es decir, UAS que usan navegación preprogramada, pero que son capaces de trasmitir información por RF)	¿Si es así, cómo?
¿Detecta el sistema UAS totalmente autónomo (es decir, UAS sin capacidades	¿Si es así, cómo?

de RF que pueden navegar sin comandos en vuelo)?	
¿Puede el sistema detectar UAS encendidos, antes que hayan iniciado el vuelo?	¿Si es así, cómo?
¿Puede el sistema detectar y geolocalizar la estación de control terrestre (GCS)?	Si es así, ¿cómo logra esto?
¿El sistema solo tiene capacidad de línea de visión (LOS)?, es decir, ¿los árboles y los edificios inhibirán las capacidades del sistema?	
¿Qué personal debe operar el sistema?	¿Qué tipo de entrenamiento es necesario para usar el sistema? ¿Qué entrenamiento está incluido?
¿Qué soporte operacional está incluido dentro del proceso de adquisición del sistema y su garantía?	¿El soporte incluye actualizaciones de software para abordar la evolución de la tecnología UAS?
¿Es el sistema una instalación fija o se puede instalar fácilmente?	¿El personal que no está familiarizado con el fabricante o vendedor del sistema, podría instalarlo fácilmente?
¿Es el sistema fácilmente transportable a cualquier entorno?	
¿Cuáles son las especificaciones o requisitos del sistema en cada punto de instalación?	Especificaciones Requisitos por tamaño (incluida la altura de la antena / sensor) Despliegue de almacenamiento físico Configuración Comunicaciones Fuente de energía Conexión a tierra eléctrica Calibración Almacenamiento físico

PARTE 3: DETECCIÓN SECUNDARIA (EO/IR o ACÚSTICOS)

Las especificaciones para sistemas EO son similares a las de cualquier cámara digital moderna; la calidad del lente, el campo de visión, las capacidades varifocales, el tamaño de píxel y la densidad de píxeles, tienen un papel en la calidad general de la imagen y su utilidad para validar elementos de interés. Algunas métricas, como la densidad de píxeles, anteriormente utilizadas para determinar la calidad de la imagen ya no son precisas: "más megapíxeles" no significa una mejor imagen. La industria de la video vigilancia utiliza una métrica comúnmente aceptada, *Pixels Per Foot* (PPF), como un nivel más predecible de calidad de imagen.

Pregunta	*Información Adicional*
¿Cuáles son las capacidades de movimiento horizontal, vertical y zoom (PTZ) de los dispositivos EO / IR?	

¿Cómo se automatizan las capacidades de PTZ en coordinación con sensores de detección primarios?	
¿Cuál es el campo de visión del dispositivo EO / IR?	
¿Qué tipos y niveles de estabilización de imagen, si corresponde, se utilizan para los dispositivos EO / IR?	
¿Cuál es la cantidad de píxeles por pie (PPF) que proporciona el dispositivo EO?	
¿Qué longitudes de onda detecta el dispositivo IR?	

PARTE 4: DATOS E INFORMACIÓN

La gestión de datos e información juega un papel crucial en los sistemas de detección UAS. Además de las "mejores prácticas" comunes para la gestión de la tecnología de la información y la seguridad de los datos, podrían considerarse otros factores, como los paneles estadísticos, la información histórica y la portabilidad de los datos, considerados de gran importancia.

Pregunta	*Información Adicional*
¿Cómo distinguirá el sistema entre UAS autorizados y no autorizados por medio de los C-UAS?	
¿Cómo el sistema recibirá por parte de las fuerzas amigas información de vuelos de sus aeronaves?	
¿El espacio aéreo del área de interés cuenta con Zonas Prohibidas, Restringidas o Peligrosas?	
¿Cómo maneja el sistema objetivos duplicados de sensores múltiples o superpuestos?	
¿Cómo se evitará la redundancia de esfuerzos al momento de emplear los C-UAS?	
¿Cómo se verifican o validan los datos de actividades sospechosas?	
¿Cómo se generan, informan y distribuyen los datos de actividades sospechosas?	
¿Cómo se gestionan los sistemas la información histórica o que proporcionan análisis estadísticos y minería de datos?	
¿Cuál es la tasa de actualización de los sensores al sistema y del sistema a la interfaz?	
¿Cuáles son las características de alerta y alarma de la interfaz?	

¿Se tiene claridad de las Reglas de Enfrentamiento en la cadena de mando?	
¿El fabricante, el vendedor o el integrador del sistema tienen acceso a los datos capturados, derivados, transmitidos o almacenados?	
¿El fabricante, vendedor o integrador del sistema tiene una solución (geolocalización) del sistema de detección?	
¿El fabricante, el vendedor o el integrador del sistema tienen la capacidad de iniciar actualizaciones de software (con o sin consentimiento)?	
¿El sistema, los componentes o el software tienen la capacidad de implementar o mantener una lista blanca de UAS sin el conocimiento del operador u organización gubernamental?	

PARTE 5: SOLUCIONES INTEGRADAS

Algunos sistemas pueden denominarse una solución integrada, que emplea múltiples tipos de tecnologías de sensores y proporciona sus datos en una única interfaz de usuario. Otros sistemas pueden proporcionar capacidades para incorporar los elementos de hardware y software existentes de una organización.

Pregunta	*Información Adicional*
Si hay varios sistemas, ¿el sistema proporciona una interfaz gráfica fusionada para el usuario con una fuente autorizada?	
¿Cómo podría integrarse el sistema durante mucho tiempo con los centros e infraestructura de operaciones de seguridad existentes, como cámaras de seguridad, conectividad de datos y sistemas de visualización?	
¿Cómo se puede integrar la información externa, como los informes del personal de tierra o las fotos, con la información del sistema?	

ANEXO 3
EJEMPLOS DE EQUIPOS C-UAS

El presente anexo incluye algunos ejemplos de sistemas C-UAS, como guía orientativa para los EAE en el estudio y selección del sistema adecuado de acuerdo a requerimientos y escenarios operativos propios de cada EAE.

Actualmente el mercado de la industria C-UAS, ofrece una gran cantidad de sistemas que cubren diferentes necesidades.

BAL CHATRI 2

El Bal Chatri 2 es una capacidad de detección pasiva de radiofrecuencia que se utiliza para detectar e identificar UAS hostiles (Ver ilustración 11). El equipo emplea un sistema de detección de radiofrecuencia definidas por software que se utiliza para detectar e identificar Aeronaves No Tripuladas. La radio puede ser configurado para detección mientras está equipado en el equipo personal o ser configurado para una ubicación fija.

Algunas de las características son:

- Alcance: 3-5 kilómetros.
- Fuente de alimentación: 1x batería PRC-148 o enchufe.
- Duración de la batería: 4 horas.
- Peso: 2,5 libras.

Ilustración 11. Bal Chatri 2

DRONE BUSTER

El Drone Buster proporciona capacidad de detección y neutralización UAS hostiles (ver ilustración 12). Es un dispositivo de ataque electrónico, portátil, que funciona con baterías y diseñado específicamente para neutralización a los UAS. La unidad explota las debilidades de los protocolos de comunicación de drones comerciales que permiten al operador interferir la señal de control, lo que obliga a la Aeronave No Tripulada a ejecutar protocolos preprogramados de "perdida de señal".

Los Drone Busters operan estrictamente según la línea de vista y requieren que el operador mantenga la vista en el objetivo durante toda la neutralización. Si hay pérdida de la línea de visión durante la neutralización, el enemigo puede recuperar el control de la aeronave. El Drone Buster está diseñado para distorsionar los UAS controlados remotamente y guiados por GPS.

Las principales características de este sistema incluyen:

- Alcance: 400 m.
- Fuente de alimentación: 1x batería recargable BB2847.
- Duración de la batería:
- Interferencia continua: 1 hora aproximadamente.
- Detección continua: aproximadamente 4-6 horas.
- Descarga completa de la batería: aproximadamente 10 días.
- Peso: 2,5 libras.

Ilustración 12. Drone Buster

MODI

El Modi es un sistema de guerra electrónica portátil que permite detectar y neutralizar (ver ilustración 13). Los sistemas Modi proporcionan capacidades integradas de guerra electrónica táctica para neutralizar una amplia gama de UAS. La unidad puede usarse únicamente como un sistema independiente, utilizando un amplificador de potencia

montado, puede usarse en un sitio fijo o en una configuración montada y desmontarse cuando sea necesario.

Las consideraciones clave para este sistema incluyen:

- Alcance: 400 m.
- Fuente de alimentación: 3 baterias BB2590.
- Duración de la batería: desconocida.
- Peso: 40,25 libras (desmontado con el pack).

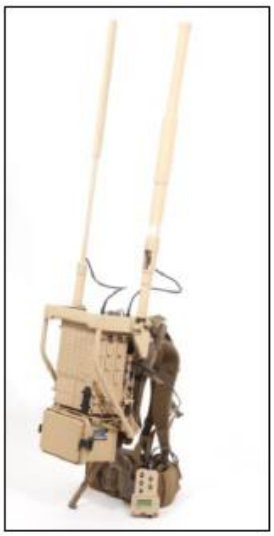


Ilustración 13: MODI

SMART SHOOTER

El Smart Shooter es una mira que se monta en sistemas de armas individuales existentes y permite al operador neutralizar UAS hostiles (ver ilustración 14). Smart Shooter es compatible con rifles militares existentes y puede montarse en cualquier riel de un sistema de armas. Para emplear el Smart Shooter, solo disparará cuando la mira esté alineada para alcanzar el objetivo, esto incluye la "dirección" de un objetivo en movimiento.

Las consideraciones clave para este sistema incluyen:

- Alcance: 120 m.
- Fuente de energía: batería de iones de litio inteligente recargable.
- Duración de la batería: 72 horas o hasta 3.600 disparos asistidos.
- Peso: 2 libras y 1 onza.

Ilustración 14: SMART SHOOTER

INTENCIONALMENTE EN BLANCO