



Artículo Nº 24 /2025

CAPACIDADES C-UAS (Counter-Unmanned Aerial Systems)

2 Parte



Por Manuel Quiñónez Sígala. General de Aviación en situación de retiro. Ex Director Ejecutivo CEEA. Profesor de la Academia de Guerra Aérea de la Fuerza Aérea de Chile. Investigador Asociado al CEEA.

11 de septiembre de 2025. 10 Min. Lectura.

Continuación:

2.- Capacidad de Reacción.

La segunda capacidad básica C-UAS esencial es la Capacidad de Reacción, que considera las actividades asociadas a la **Defensa e Interceptación**, de uno o más drones, una vez que han sido clasificados como de riesgo o amenaza.

a.- Acciones de Defensa Pasiva contra Drones.

Dentro de las acciones de **Defensa Pasiva** contra drones, se cuentan las acciones de protección física, tendientes a minimizar las vulnerabilidades materiales de los elementos protegidos y varían dependiendo de la naturaleza civil o militar de las acciones.

En el caso de las instalaciones militares, especialmente las bases aéreas, la protección más adecuada es el empleo de shelters o refugios endurecidos, que mitigan y disminuye los riesgos de los ataques directos con drones.

Las acciones de defensa del tipo pasivo son efectivas, siempre y cuando se cuenta con un sistema de alerta efectivo, es decir, que integre de los sistemas de detección e identificación de drones con los equipos de los Sistemas de Mando y Control existentes.

Para los efectos de una efectiva integración, deben procurarse sistema que utilicen protocolos de comunicación interoperables y automatizados.

b.- Acciones de Interceptación de Drones.

En el caso de las actividades asociadas a la Interceptación de Drones, éstas se refieren a elementos que permiten clasificar los drones, entregar las alertas correspondientes y activar la fase siguiente de neutralización de drones, de ser necesario, de acuerdo a la naturaleza o tipo de dron que constituye la amenaza o riesgo.

Para identificar drones, se requiere normalmente una suma de las capacidades de detección, cuyos sensores transmiten la data a un sistema o software central, que el capaz de distinguir entre los drones en uso por las fuerzas propias, y aquellos no autorizados o catalogados como de riesgo o amenaza. Ello requiere de altos niveles de integración, que

permita la representación de la situación para un correcto *Drone Situational Awareness*, conducentes a una apropiada alerta de defensa pasiva y a las acciones de interceptación.



*Representación gráfica de la Capacidad de Reacción antidrones.
Confección del autor.*

Para los requerimientos de integración, existen empresas en el país con una amplia experiencia en sistemas de comunicaciones y de mando y control, las que unidas a las de los proveedores de los sistemas de detección e interceptación, permitirían asumir estas responsabilidades, constituyéndose en una oportunidad de generar capacidades a nivel nacional.

Al igual que en las capacidades de integración de sensores y equipos, existe una amplia gama de equipos y empresas que pueden cubrir la capacidad de reacción mediante alertas, a fin de asumir la interceptación y posterior neutralización o captura. Las alertas son normalmente cubiertas por los sistemas de comunicaciones ya existentes en las instituciones. Sin embargo, se debe buscar la capacidad de configurar sistemas especiales multibandas y encriptados, de acuerdo a las necesidades particulares de cada institución.

3.- Capacidad de Neutralización.

La capacidad operacional básica final de las actividades C-UAS, es la Capacidad de Neutralización, que considera las actividades asociadas a la ***Neutralización, inhibición, destrucción o captura*** de uno o más drones clasificados como riesgo o amenaza.

Las soluciones de neutralización, inhibición, destrucción o captura de drones disponibles incluyen soluciones del tipo ***soft-kill*** (no cinéticas) y ***hard-kill*** (cinéticas).

Las soluciones soft-kill implican métodos que no dañan físicamente a los drones, tales como los sistemas de interferencia de RF o de *hackeo* de drones.

Por otra parte, las soluciones hard-kill afectan físicamente al dron mediante otro objeto, un proyectil o por energía dirigida. Estas soluciones van desde

“drones caza drones”, hasta soluciones como equipos láser y el uso de municiones de distintos tipos y calibres.

Las soluciones *soft-kill* suelen conllevar menos riesgos de daños colaterales debido a su naturaleza no cinética y son más sutiles y discretas en su funcionamiento. Como resultado, los métodos cinéticos y de *hard-kill* se reservan casi exclusivamente para el uso militar y de fuerzas de seguridad estatales, con pocas excepciones.

Otro tema presente en las capacidades de neutralización de drones, es el aspecto legal. En forma especial, debe asegurarse la correcta asignación de autorizaciones para contrarrestar el accionar de drones en tiempos de paz, lo que puede variar entre los países o por el tipo de restricción impuestas en zonas críticas, tales como aeropuertos, alrededor de la infraestructura crítica o en eventos públicos masivos.

Aunque se utilizan en forma generalizada, incluso los métodos no cinéticos requieren de diferentes niveles de autorizaciones para operar, lo que se aplica tanto para civiles como para las agencias gubernamentales.

En el caso de los drones que son piloteados por un operador remoto (RPAs), se utiliza las emisiones electromagnéticas asociadas a su operación, tanto para ayudar a su detección y localización, como para su neutralización (también llamadas técnicas de inhibición de RF), llegando incluso a la detección y localización geográfica del propio operador.

Las técnicas más comunes contra este tipo de drones lo constituyen el *Jamming* (interferencia electromagnética) de su señal de guiado, el *Spoofing* (o engaño de la señal GPS que recibe el dron, afectando su navegación) y el *Hacking*, que permite al interceptor interferir en los códigos de comando contenidos en la señal de guiado, pudiendo llegar a tomar el control de vuelo completo del dron afectado.

El detalle de las técnicas de neutralización de drones (especialmente de los sUAS) se comentan en los puntos siguientes.



Gráfica: Representación de la capacidad de Neutralización/Inhibición de drones.
Confección del autor.

a.- Neutralización o Inhibición por Interferencia Electromagnética (Jamming).

Los inhibidores de RF (o *Jamming* de RF), transmiten en la misma frecuencia que utiliza un UAS para comunicarse con el controlador u operador. Cuando la señal de interferencia es más fuerte en el UAS que la señal del controlador al dron, el UAS pierde su conexión y se ve obligado a entrar en un protocolo de emergencia preestablecido para volar de regreso a su punto de partida, flotar en vuelo estacionario o aterrizar.

Los UAS comerciales más comunes se comunican dentro de bandas de frecuencia conocidas, tales como las de 2,4 GHz y 5,8 GHz. El UAS utiliza estas frecuencias para comunicarse con su controlador y para la visualización de vídeo en primera persona (FPV). Otras bandas de frecuencia de RF menos comunes utilizadas comercialmente incluyen las de 433 MHz y 915 MHz ISM.

El diseño del inhibidor puede ser direccional u omnidireccional (360 grados). La interferencia omnidireccional proporciona una cobertura de defensa más amplia, mientras que las soluciones direccionales o basadas en sectores ofrecen más precisión y mitigan las interferencias colaterales o no deseadas.

Las certificaciones de seguridad son un aspecto fundamental a considerar para la selección de los equipos de interferencia. Los equipos más baratos pueden exponer al operador a un exceso de energía de RF, poniendo con el tiempo en riesgo su salud¹. En el mejor de los casos, debe considerarse contar con equipamiento y laboratorios propios, que permitan asegurar una certificación de seguridad acreditada de primera fuente.

Los inhibidores suelen integrarse con los dispositivos de detección de RF, como un sólo dispositivo que comparte las mismas antenas, lo que produce una solución compacta y totalmente integrada de detección y desactivación.

Si bien no es una panacea para todos los tipos posibles de drones, la interferencia de señales está considerada como una de las técnicas más costo-efectivas en el ámbito las capacidades C-UAS². Lo anterior significa, que esas capacidades pueden desplegarse en un número mucho mayor de unidades de nivel táctico, en lugar de limitarse sólo a algunas unidades más especializadas.

Sin embargo, hay que tener presente que esa técnica no cubre la detección y posterior neutralización de los llamados drones autónomos, los que son cada vez más comunes en el ámbito de las amenazas militares.

¹ Op. Cit. C-UAS Factbook, pág. 22.

² Ibid.

b.- Neutralización o inhibición por Interferencia de la señal GPS (Spoofing) que reciben los drones.

El GPS es el sistema GNSS más conocido, pero también existen a nivel global los sistemas GLONASS (ruso), Galileo (Europa), BeiDou (chino), QZSS (japonés) y NavIC (indio).

En tal sentido, los drones comerciales y de alto consumo suelen venir con múltiples capacidades GNSS.

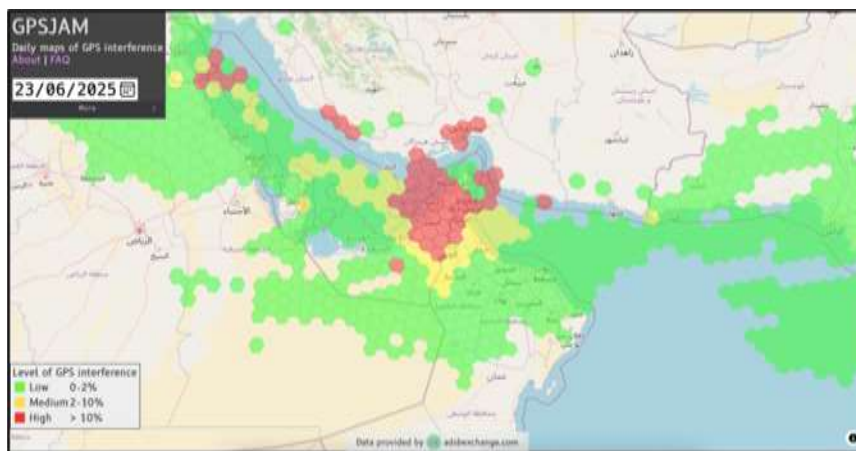


Imagen: Visualización de la capacidad de interferencia de GPS o Spoofing de área, en preparación a los ataques a la Base Aérea de Al-Udeid en Qatar por parte de Irán³.

Si se interfiere la frecuencia de RF de un dron, este aún puede utilizar GNSS para volar de regreso a su punto de origen o continuar a lo largo de una ruta de navegación preprogramada.

Al interferir tanto la señal de RF como la de GNSS, el UAS se separa de sus enlaces de comunicación y navegación y no puede volar a casa ni continuar su trayectoria de vuelo preprogramada.

Los equipos comerciales de interceptación o inhibidores de drones suelen contar con una capacidad adicional de spoofing de señal GNSS, que cubre una o más fuentes de señal de navegación. Por otra parte, dependiendo de las capacidades del dron, una vez interferido éste puede intentar aterrizar en el lugar o flotar hasta que se agoten las baterías.

c.- Neutralización o inhibición por suplantación de identidad del operador, manipulación de protocolos o interferencias cibernéticas (Hacking).

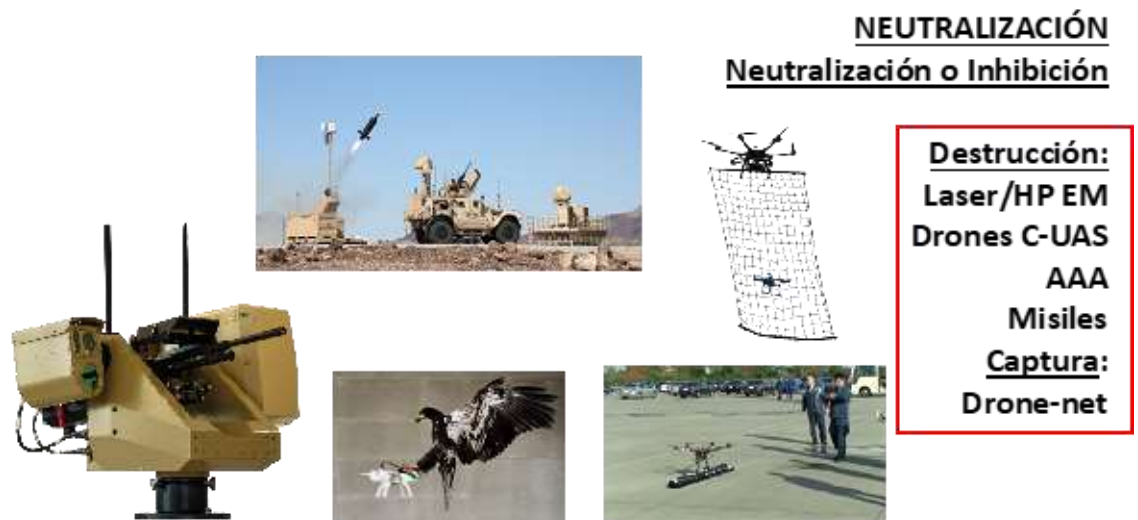
La suplantación de identidad o "*hacking*", implica una forma de manipulación del protocolo de guiado. Este método incluye imitar al controlador y obtener el control del dron actuando como controlador. Cuando tiene éxito, esta técnica permite que el sistema redirija el dron, lo que puede ser de mucha utilidad, especialmente para análisis del operador y

³ Fuente: <https://gpsjam.org>.

de la amenaza. La suplantación de identidad también puede incluir la suplantación de la señal GNSS, lo que desvía efectivamente la dirección del dron.

Una limitación importante de este enfoque, es que las técnicas de suplantación de identidad no son eficaces contra todos los tipos de drones, por lo que siempre existe el riesgo de penetrar el sistema de protección.

Otro aspecto a considerar, son los aspectos legales respecto de la manipulación de protocolos, la que puede requerir permisos o autorizaciones judiciales para su empleo.



*Representación gráfica de la capacidad de Destrucción o Captura de drones.
Confección del autor.*

d.- Interceptación de Drones mediante Energía Irradiada (Directed Energy).

Los métodos de interceptación y destrucción de drones mediante energía irradiada dirigida incluyen sistemas láser y de microondas de alta potencia. Estos métodos se encuentran en sus primeras etapas desarrollo y actualmente se está evaluando para aplicaciones militares más masivas, siendo su mayor desventaja los costos de fabricación y mantención.

e.- Interceptación y captura de drones mediante “Drones C-UAS”.

Los drones contra-drones (*Drones C-UAS*) son por lo general del tipo autónomo, y utilizan la energía cinética para derribar en el aire a los drones objetivos (estilo *kamikaze* aire-aire). También, se han desarrollado “drones caza drones”, que atrapan o inutilizan los drones objetivo mediante el uso de redes colgantes (*Drone-net*), o redes disparadas por un dron hacia el objetivo. Esta técnica también se utiliza desde tierra, mediante cañones que usan municiones modificadas tipo red.

Estas técnicas tienen dificultades para escalar, especialmente contra enjambres de drones, además de que el enfoque kamikaze agrega un alto riesgo de daños colaterales o lesiones en caso de ocurrir sobre público.

f.- Sistemas combinados de interceptación y neutralización C-UAS.

Al igual que con los métodos de detección, la interceptación y neutralización de drones mediante el uso de defensas multi-capas, proporciona robustez y efectividad contra diversas amenazas UAS, y son altamente recomendables.

Los enfoques combinados o multi-capas pueden incluir opciones de eliminación tipo *soft-kill* y de *hard-kill*, de manera de optar por múltiples estrategias para que el usuario pueda emplear la contramedida ideal basada en los cambios en tiempo real dentro del entorno operativo u objetivo, tal como se verá en los puntos siguientes.

III. CAPACIDADES C-UAS, DE ACUERDO A LOS ESCENARIOS PREVISTOS.

Como se estableció en los antecedentes, este artículo responde a la necesidad de conocer respecto de las capacidades C-UAS, y está orientado específicamente contra las actividades de los llamados drones pequeños o sUAS (*small UAS o small UAV*).

Basado en ello, en este capítulo se establecen recomendaciones preliminares para obtener las capacidades C-UAS, de acuerdo con distintos escenarios. Lo anterior, cubriendo las diferentes capacidades básicas, representadas por las fases de detección, reacción identificación y de neutralización o destrucción.

En cuanto a los sistemas que brindan soluciones prácticas, muchos países han optado por incorporar equipos de interceptación y neutralización de drones móviles costo-efectivos, que pueden actuar en forma conjunta con los radares de detección y los sensores de detección de RF y ópticos, utilizando protocolos comunes y probados, reduciendo tiempos y costos de integración.

Asimismo, a fin de lograr una movilidad que permita cubrir áreas mayores o puntos fijos, se ha recurrido al empleo de sistemas de interceptación de drones del tipo Manpack (hombros portados) y de mano (o de empañadura), que dispongan, en el mismo equipo, de las técnicas de *Jamming* (interferencia electromagnética) y de *Spoofing* (o engaño de la señal GPS) que recibe el dron, afectando su navegación.

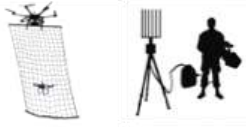
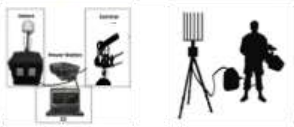
Para efectos de la incorporación de capacidades C-UAS contra drones pequeños, es importante tener en cuenta las consideraciones del **escenario previsto para su empleo**, el que puede variar desde el escenario menos complejo de protección de instalaciones fijas o de autoridades, pasando por las Operaciones Militares Distintas de la Guerra (MOOTW, por sus siglas en inglés), llegando hasta las operaciones C-UAS en situaciones de Crisis o Conflictos.

Los escenarios descritos influyen en las medidas a adoptar en la detección, reacción y neutralización o inhibición de los drones, especialmente en los tiempos de reacción disponibles, reglas de enfrentamiento asociadas, y el análisis de riesgo de daño colateral o sobre la población o instalaciones críticas, lo que en muchos casos condiciona el uso de opciones cinéticas.

Estas variables, a su vez, condicionan el tipo de **sistemas de mando y control** a emplear, tanto en equipamiento, conectividad y niveles de decisión requeridos.

Paralelamente, es necesario tener en cuenta el **tipo de emplazamiento requerido**, el que puede ser del tipo de emplazamiento fijo, usado principalmente para protección de bases o infraestructura crítica en general; de emplazamiento móvil, basado en vehículos, barcos y/o aeronaves, aplicable a grandes extensiones o protección de fuerzas en movimiento, y; el emplazamiento portátil o de empuñadura, normalmente empleados por fuerzas de orden y seguridad para protección de puntos fijos o en la protección de autoridades importantes.

Teniendo en cuenta las consideraciones anteriores, así como los antecedentes y especificaciones genéricas de los sistemas de detección, reacción y neutralización mencionados en el escrito, se llegó a la tabla siguiente, en donde se señalan los escenarios previstos y los distintos tipos de sistemas y equipamiento C-UAS recomendado para la concreción de las Capacidades C-UAS básicas contra drones pequeños.

TIPO DE EQUIPAMIENTO RECOMENDADO	PROTECCIÓN DE INSTALACIONES	MOOTW	CRISIS O CONFLICTOS
Radar de Detección de Drones: - Radar - EO/IR - RF	 Radar 2D Radar 3D	 Radar 3D IR/EO	 Radar 3D IR/EO
Integración Situación Aérea Local y a la Defensa Aérea del Teatro/Zona de Operaciones	 CIS	 CIS & C2	 CIS & C2
Sistemas Anti Drones Electrónicos y de Captura, Fijos y Móviles	 Drone-net RF/DF Portátil	 RF/DF & C2 Móvil RF/DF Portátil	 RF/DF & C2 Móvil RF/DF Portátil
Sistemas Anti Drones Tipo AAA y MANPADS factibles de integrar a nivel nacional			 AAA MANPADS

NOTA: Ilustraciones son genéricas y no representan a ningún sistema o empresa en particular.

Tabla: Recomendación de Tipo de Equipamiento Recomendado para Capacidades C-UAS básicas contra drones pequeños. Confección del autor.

IV. CONCLUSIÓN.

Este artículo pone en relevancia el aumento exponencial a nivel mundial en la fabricación y operación de drones aéreos (*Unmanned Aerial Vehicles*, UAV o *Unmanned Aerial Systems*, UAS) con capacidades militares, así como la fácil disponibilidad de estos ingenios a nivel comercial, que incide directamente en la vulnerabilidad a la que se enfrentan las fuerzas militares, sus instalaciones y la infraestructura crítica, tales como puertos y aeropuertos, sistemas de alimentación eléctrica, de combustibles, etc.

Sin duda, el desafío para la seguridad militar que representan los UAS es un "problema perverso" que no puede resolverse con una única solución. La creciente proliferación de drones, tanto militares como comerciales, y su adaptación a nuevos roles operativos, exige un cambio fundamental en la forma en que las organizaciones militares y civiles abordan la seguridad. La cooperación, la inteligencia, la adaptación legal y tecnológica, y una visión proactiva de las autoridades de defensa son pilares indispensables para "domar" la amenaza y mitigar sus impactos.

La velocidad de desarrollo de los UAS requiere que las capacidades C-UAS no se queden atrás, ya que, de lo contrario, las naciones y las Fuerzas Armadas pueden enfrentar una clara y decisiva desventaja en sus próximas operaciones.

