UAS EN EL CONFLICTO MODERNO: UNA VISIÓN AMPLIADA

Maximiliano Larraechea Loeser
Director Ejecutivo del Centro de Estudios Estratégicos y Aeroespaciales

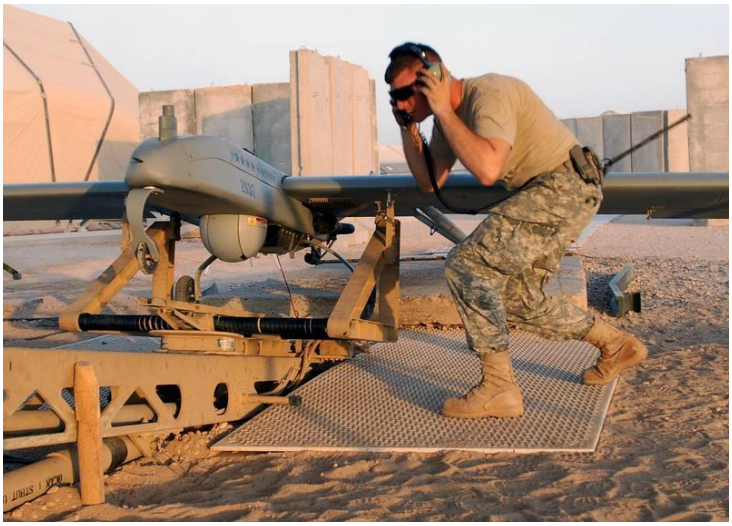
INTRODUCCIÓN

Los sistemas de aeronaves no tripulados (UAS) se han desplegado en todas las instituciones militares, comprendiendo desde los micro-UAS de mano hasta sistemas tácticos de tamaño mediano y aeronaves pilotadas (RPA) totalmente desarrolladas. Al mismo tiempo, el mercado civil ha sido testigo de un crecimiento exponencial de aparatos cada vez más pequeños, destinados al uso público y el recreativo. Sin embargo, el ámbito del uso recreativo y su desarrollo increíblemente rápido, ha llamado la atención de las instituciones de aplicación de la ley y a las comunidades de protección de la fuerza militar, debido al aumento del uso indebido de "drones" "comerciales fuera de la plataforma" (COTS) cerca o en aeropuertos, eventos públicos e instalaciones militares. En ese sentido, Chile a través de su Dirección General de Aeronáutica Civil dependiente de la Fuerza Aérea, fue pionero en el mundo al implementar una norma que regula el uso de RPAs en espacios públicos, pero eso es claramente insuficiente para dar por solucionado el problema.

A nivel mundial, varios actores de la industria reaccionaron a la demanda emergente de capacidades para defenderse contra estos COTS UAS mediante el desarrollo de sensores y medios activos Contra-UAS (C-UAS). Estos sistemas están diseñados específicamente para detectar, rastrear y enganchar aparatos voladores bajos, lentos y pequeños (LSS), que van desde sistemas portátiles hasta modelos montados en vehículos. Los Estados Unidos representan el más completo avance en el tratamiento de este problema. En Europa, la OTAN también reaccionó a esta nueva amenaza realizando una serie de estudios centrados

en la defensa contra las amenazas aéreas de LSS y estableciendo un Grupo de Trabajo dedicado a estudiar el posible uso terrorista de UAS. Hoy, todas las potencias medianas desarrollan capacidades en esta área, por lo que conocen sus cualidades y pueden prever la amenaza que representan empleadas en contra suya.

La tecnología se está desarrollando rápidamente y en muchos casos, más rápido de lo que la industria de defensa puede reaccionar. Por ejemplo: muchas contramedidas "tradicionales" contra pequeños UAS se basan en la interferencia electrónica del enlace de comando y control entre el "dron" y su control remoto. Sin embargo, muchos productos COTS actuales pueden navegar de forma autónoma a una determinada coordenada o pueden controlarse a través de una red GSM o 4G desde el teléfono celular del operador. Estas características hacen que la interferencia sea completamente inútil, ya que el enlace de Comando y Control (C2) ya no es necesario para navegar, o, debido a restricciones de tiempo de paz, las frecuencias que requerirían bloquearse a menudo están prohibidas para otros fines y se hace legalmente casi imposible accionar en su espectro, ya que son utilizadas por el público. En un futuro muy cercano, los UAS podrán incorporar Inteligencia artificial (AI), tomando sus propias decisiones una vez lanzados al aire y no requerirán enlaces con operadores para ello. Además, un único enfoque en el extremo bajo, lento y pequeño del espectro C-UAS cubre solo una fracción de la tecnología UAS actual y excluye la mayoría de las aplicaciones militares. Se puede esperar que los eventuales adversarios empleen UAS adquiridos o desarrollados por ellos mismos, al mismo nivel de tecnología y bajo principios operativos comparables, como los propios. En consecuencia, se necesita anticipar el futuro uso enemigo de UAS en los mismos conjuntos de misiones que con los UAS amigos, cubriendo el espectro que va desde la Inteligencia, Vigilancia y Reconocimiento hasta ataques aéreos no tripulados, conducidos en Line of Sight (LOS) así como operaciones Beyond Line of Sight (BLOS), utilizando el espectro electromagnético y el dominio espacial en forma tanto o más efectiva que nosotros.

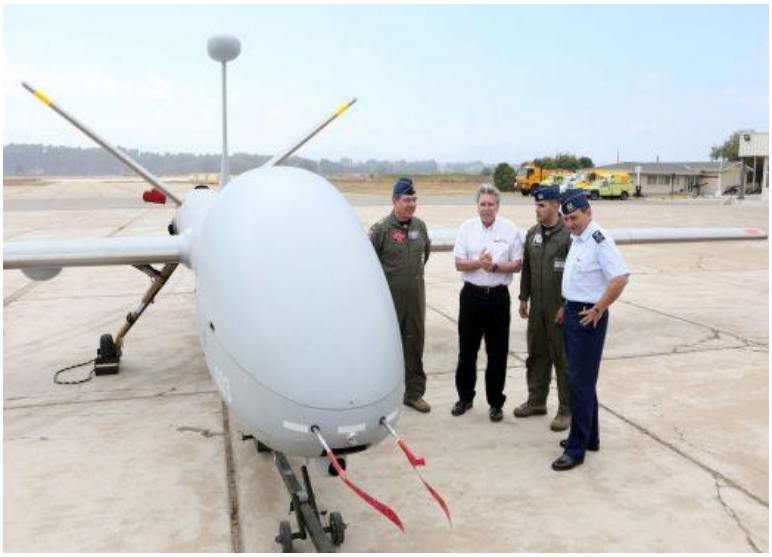


A continuación, se expone brevemente un espectro de consideraciones de empleo contra UAS y una explicación de por qué el enfoque teórico actual concentrado en RPAs de vuelo bajo, lentos y pequeños, aunque inminente y esencial, no es suficiente para cubrir todos los aspectos de la defensa ***contra*** posibles enfrentamientos de UAS adversarios.

EL ESPECTRO DEL EMPLEO CONTRA LOS SISTEMAS DE AERONAVES NO TRIPULADAS

Para comprender el espectro completo de contrarrestar UAS , y aquí recalcamos que la "S" justamente expresa la importancia de un "sistema", es importante tener en cuenta que centrarse exclusivamente en la aeronave no tripulada (UA) o "dron" no proporciona un panorama completo. Los UAS se agrupan en varias categorías y consisten en numerosos componentes, dependiendo de su tamaño y aplicación, los que pueden ser objeto de ataque para la inutilización del sistema.

1.- Categorías de sistemas de aeronaves no tripuladas. Occidente clasifica a los UAS en tres clases, que van desde la Clase I para las micro, mini y pequeñas, continuando con la Clase II para sistemas tácticos de tamaño mediano, hasta la Clase III para gran autonomía a altitud media (MALE) y gran altitud y gran autonomía (HALE). Al observar diferentes clases, su aplicación, tamaño y altitud de operación, se puede concluir que contrarrestar este espectro de UAS requiere una multitud de enfoques diferentes y específicos para cada clase. Como regla general, cuanto mayor sea el UAS, mayor será su dependencia de infraestructuras como refugios, pistas, aeródromos o aeropuertos. Lo mismo es cierto para la logística como combustible, municiones y mantenimiento. Finalmente, los sistemas no tripulados siempre requieren personal para operarlos. Esto puede variar desde un solo individuo que opera un pequeño dron hasta múltiples tripulaciones que se rotan en turnos para sistemas más grandes, como vemos en Nevada, EE.UU o en Europa con sistemas que opera la OTAN. Los UAS militares de clase superior que realizan misiones de inteligencia o reconocimiento también requieren una cantidad significativa de personal de Procesamiento, Explotación y Difusión para analizar la información proporcionada por el UAS.



2.- Componentes del sistema de aeronaves no tripuladas. La configuración básica de un UAS pequeño consiste en un operador, un control remoto, un enlace y el avión o "dron" en sí. Los sistemas más grandes también pueden incorporar una estación de control de tierra (GCS) dedicada para el lanzamiento y la recuperación, así como un elemento de control de misión (MCE) para llevar a cabo la operación. Los sistemas más grandes suelen utilizar comunicaciones BLOS (Beyond Line Of Sight) con espacio habilitado para Comando y Control (C2) y enlaces de datos. Los GCS y MCE consisten en infraestructura física, como camiones y contenedores, que generalmente alojan el hardware y el software de los computadores asociados que, a su vez, ejecutan las aplicaciones necesarias para operar el sistema en general.

3.- Posibles puntos vulnerables

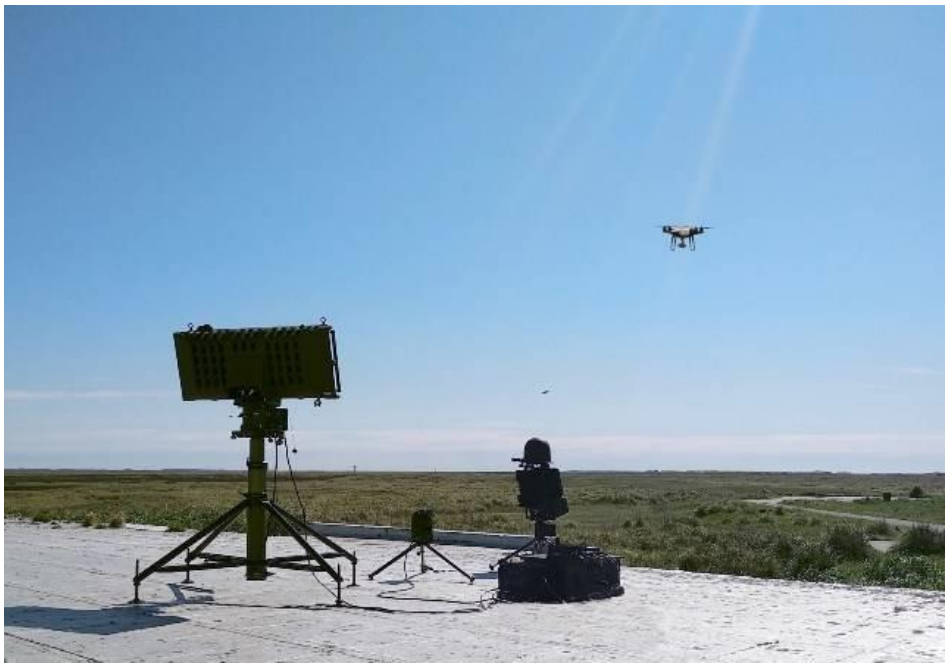
Dependiendo del componente en sí, el dominio en el que está operando y su distancia potencial a las fuerzas propias, se presentan diferentes puntos que se visualiza a priori como vulnerables como opciones para el empleo de contramedidas físicas, electrónicas o informáticas. Si bien estos puntos vulnerables pueden abordarse mediante las misiones descritas en las secciones que se detalla a continuación, todas deben complementarse entre sí y contribuir a lo que podríamos denominar "un esfuerzo integral multidominio Contra-UAS".

4.- Algunas consideraciones de empleo, previstas en este desafío.

a.- Protección de fuerza (FP). Para las Unidades de Protección de la Fuerza, debe tenerse en cuenta que muchos UAS están fácilmente disponibles como productos COTS para cualquier persona y representan una amenaza inminente para la infraestructura pública crítica y las instalaciones militares. Las medidas de protección de la fuerza tradicionales, que garantizan la seguridad de las fuerzas amigas y la infraestructura crítica, suelen estar muy localizadas y centradas en el área que requiere protección, como asimismo focalizadas contra incursiones terrestres convencionales o Fuerzas Especiales y no han asumido protocolos específicos contra ataques de UAS.

Los obstáculos naturales y creados por el hombre, como los árboles o los edificios, pueden cubrir una incursión de pequeños UAS y retrasar significativamente la detección de estos objetos en el área, acortando aún más el tiempo de reacción disponible. Las medidas de protección de la fuerza deben estar dirigidas principalmente a negar el acceso de los UAS al área protegida. Sin embargo, también puede ser deseable capturar de forma segura el UAS con fines de inteligencia.

b.- Defensa Aérea (AD). Los UAS más grandes pueden operar a altitudes de hasta 30,000 pies y, en algunos casos, incluso más alto. La sección transversal de radar (RCS) de estos UAS es comparable a cualquier otra aeronave con características *Stealth*, por lo tanto la mayoría de los sistemas de defensa aérea y de misiles (AMD) pueden detectarlos y activarlos. Sin embargo. La munición moderna de superficie a aire no es barata, es generalmente escasa y está diseñada para atacar objetivos de alto valor. Grandes cantidades o un enjambre de UAS de bajo costo pueden cambiar rápidamente la relación costo-beneficio de la AMD tradicional y hacer que los sistemas actuales sean ineficientes. ¿Lanzará usted un misil de mediano alcance contra un *Dron*?



Por otra parte, la defensa aérea de corto alcance, incluyendo la artillería antiaérea, puede y debiera proporcionar una defensa efectiva, pero también eficiente, contra los UAS de vuelo a baja altitud.

c.- **Interdicción Aérea (AI).** Es posible en muchos casos, es factible la interdicción de un UAS, esto es, la inutilización o destrucción de un elemento del sistema que haga imposible que entre en contacto con nuestras fuerzas. El lanzamiento y recuperación de UAS más grandes generalmente se realiza desde un GCS dentro o cerca del área de la misión. El GCS puede ser móvil y montado en un camión o estacionario cuando se coloca en el suelo; por ejemplo, cerca de un aeródromo. En cualquier caso, el Elemento de Lanzamiento y Recuperación (LRE) de UAS más grandes es un objetivo de alto valor, ya que a menudo es responsable del lanzamiento y recuperación de varios UA. La eliminación de un LRE probablemente detendrá las operaciones de UAS en el área respectiva ya que los nuevos UAS ya no se pueden lanzar y los ya en operación no se pueden recuperar de manera segura.

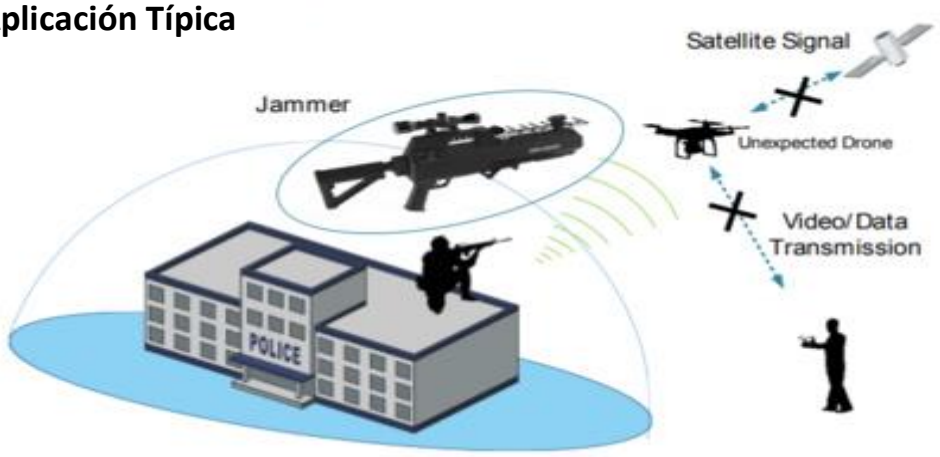
d.- **Empleo de Fuerzas de Operaciones Especiales.** Una vez en el aire, los sistemas más grandes a menudo se pueden transferir del LRE a un MCE y operar BLOS a través de comunicaciones satelitales (SATCOM). El MCE se puede ubicar lejos del área de la misión, probablemente en el interior del territorio adversario. Las Fuerzas Especiales pueden emplearse como un medio para atacar el MCE del enemigo, eliminar los nodos terrestres SATCOM que son esenciales para las operaciones de UAS BLOS, o incluso eliminar combatientes adversarios como son los miembros de la tripulación de UAS.

e.- **Ciberoperaciones.** Los UAS dependen completamente de sus sistemas informáticos, tecnología de la información y conectividad de red. Las estaciones de control, especialmente dentro de instalaciones fijas como un MCE, son potencialmente vulnerables a los ataques a través del ciberespacio, explotando las vulnerabilidades de seguridad de su hardware y software, pero también aprovechando la falla humana. Es probable que un COTS UAS operado a través de una red GSM solo sea accesible a través del dominio del ciberespacio, ya que las contramedidas en el espectro electromagnético pueden estar fuera nuestro alcance.

Los UAS más grandes requieren una cantidad significativa de hardware, software y redes para operar. Por lo tanto, el dominio del ciberespacio puede ofrecer posibles contramedidas capaces de lograr que toda la red y la infraestructura de comunicaciones de uno o más sistemas no tripulados no funcionen. Sin embargo, las contramedidas en el dominio del ciberespacio pueden requerir más que solo una postura defensiva. La colocación preventiva y encubierta de “puertas traseras” (Backdoors) en sistemas informáticos adversos, puede garantizar el acceso a estas redes cuando sea necesario y probablemente sea la única forma de prepararse y reaccionar rápidamente ante una amenaza inminente de UAS

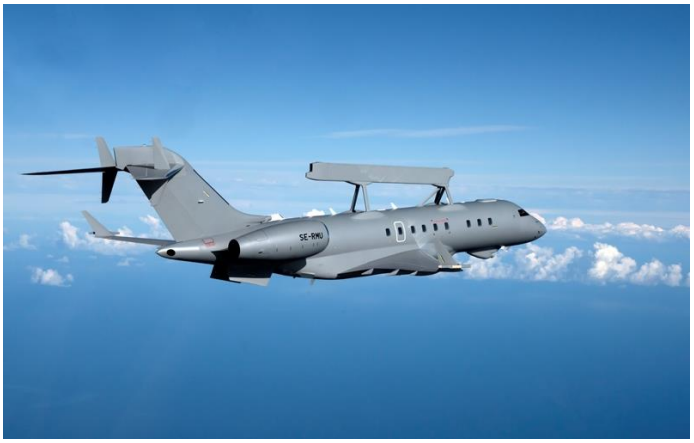
f.- **Operaciones de Guerra Electrónica (GE).** El Mando y Control (C2) del UAS se realiza a través de transmisiones de radio LOS o BLOS y, por lo general, también depende de las señales de posición, navegación y sincronización (PNT). Las operaciones de GE se pueden usar en todos los niveles de UAS para obstaculizar e interrumpir las transmisiones C2 y PNT o incluso para falsear información PNT para desviar o aterrizar el UAS.

Aplicación Típica



Sin embargo, la guerra electrónica "tradicional" tiene sus límites con los modelos modernos de UAS, que son capaces de volar de forma autónoma y ya no dependen de enlaces de datos continuos. Las próximas armas de energía dirigida, como las microondas de alta potencia o los láseres de alta energía, pueden agregar capacidades a la cartera electromagnética y podrían usarse para inutilizar las cargas útiles de los sensores o destruir un UA.

g.- **Inteligencia, Vigilancia, Reconocimiento (ISR).** Detectar los UAS en vuelo, es a menudo el primer paso para defenderse de ellos. Se puede detectar un UAS más grande incluso con el uso de sistemas de radar convencionales, mientras que los UAS del tipo LSS (los pequeños) requieren un sistema más especializado para distinguirlos del "ruido" generado, por ejemplo, por hojas y pájaros. Sin embargo, aparte de emplear las capacidades ISR para la vigilancia del espacio aéreo y la situación de superficie, la identificación confiable de un UAS intruso y sus capacidades, así como la identificación del origen de la transmisión C2, es crítica para seleccionar las contramedidas apropiadas. Por ejemplo: esto incluye información sobre las capacidades y el nivel de autonomía del UAS, ubicaciones de LRE y MCE adversarios, así como los activos y frecuencias de SATCOM utilizados. Los sistemas Contra-UAS deben ser alimentados con esta información, preferiblemente en tiempo real, para procesar una solución adecuada.



h.- **El dominio espacial.** Las comunicaciones basadas en el espacio son una parte esencial de las operaciones de los UAS BLOS. Pero los aparatos de origen comercial o COTS UAS también utilizan señales posición, navegación y sincronización o PNT proporcionadas por las respectivas constelaciones de satélites. Dentro de los límites del "Tratado del Espacio Exterior", las contramedidas contra las comunicaciones basadas en el espacio y el PNT

pueden ser una opción legítima para defenderse contra toda una flota de adversarios UAS. Esto no requiere necesariamente de empleos cinéticos con armas antisatélite. De hecho, las capacidades de interferencias terrestres o espaciales podrían ser efectivas sin arriesgar grandes cantidades de chatarra espacial que podrían inutilizar órbitas enteras para la humanidad.

5.- Algunas Consideraciones legales

Las formas de empleo para UAS van desde empleos públicos y recreativos hasta misiones militares, incluidos los ataques aéreos. En consecuencia y dependiendo de su uso, la defensa contra estos sistemas se rige por el derecho nacional o internacional, y el marco legal que debe aplicarse también depende de si es tiempo de paz o de guerra. En nuestro país, la reglamentación aeronáutica considera la aplicación de restricciones al empleo civil, sobre todo en áreas públicas, pero la escasa capacidad de fiscalizar la comercialización y el empleo de los sistemas más livianos supone un problema a enfrentar. Defenderse contra UAS no es solo un requisito de tiempo de guerra. Los incidentes frecuentes en otras latitudes ya han demostrado que los "drones" COTS pueden volar fácilmente al espacio aéreo restringido y pueden detener las operaciones de vuelo de todo un aeropuerto. Hemos tenido incidentes menores, casi anecdóticos, en el Palacio de la Moneda y en alguna Base Aérea. Es solo una cuestión de tiempo antes de que se observe un incidente grave en instalaciones militares, como por ejemplo en bases aéreas, cuarteles o campos de entrenamiento militar.

Dependiendo del país y su legislación nacional, que es aplicable durante el tiempo de paz, las circunstancias pueden prohibir ciertos tipos de contramedidas y limitar las opciones para defenderse contra los UAS. Estas contramedidas posiblemente prohibidas incluyen el ataque cinético en contra de los sistemas no tripulados en el aire, la interferencia de frecuencias utilizadas públicamente, como las redes GSM o inalámbricas, o la interferencia con las señales comerciales PNT. En general, se puede suponer que contrarrestar los UAS en tiempos de paz estará sujeto a una multitud de restricciones civiles que pueden o no aplicarse completamente en un escenario de conflicto. La doctrina C-UAS y las Tácticas, Técnicas y Procedimientos (TTP) deben incluir estos detalles y adherirse a los entornos legales individuales.

En tiempos de paz, la responsabilidad de la defensa contra "drones" y UAS de bajo peso, generalmente recae en las agencias de aplicación de la ley civil. Sin embargo, las responsabilidades pueden superponerse cerca de las instalaciones militares y la infraestructura crítica. Además, los organismos encargados de hacer cumplir la ley pueden requerir apoyo militar, ya que el equipo para detectar, identificar y atacar a los UAS muchas veces solo es provisto por las fuerzas armadas. Por lo tanto, la estrecha cooperación y coordinación entre las agencias civiles de aplicación de la ley y las fuerzas armadas son esenciales para un enfoque integral de Contra-UAS. Esta es una más de las múltiples razones que hacen imperativo que las Políticas Públicas involucradas (por ejemplo, Defensa vs Ministerio de Transportes y Telecomunicaciones) sean coherentes entre sí y coordinadas desde la conducción política.

La legislación interna dedicada (como nuestro Código Aeronáutico) también puede ayudar a defenderse contra los UAS de tal manera que se requiera que los "drones" livianos del tipo COTS transmitan una señal de identificación y posicionamiento (Transpondedor) comparable al tráfico aéreo y marítimo civil regular. Algunos fabricantes ya equipan sus drones voluntariamente con transpondedores que proporcionan esta información en una radiofrecuencia separada y sin cifrar. Por supuesto, esto no evitará el abuso criminal o terrorista de estos sistemas, pero si hubiera legislación vigente, cualquier sistema que no proporcione una señal de transpondedor podría clasificarse como potencialmente hostil.

6.- Seguridad pública y daños colaterales. La protección de los civiles contra los daños, es un principio elemental del derecho internacional y del derecho interno. Por lo tanto, la defensa contra UAS requiere la consideración de los riesgos potenciales para la vida humana, tanto en tiempos de paz como en tiempos de guerra. Los civiles pueden estar en peligro de ser afectados por el uso medidas cinéticas como el derribo de UA o un ataque a sus instalaciones terrestres, en la misma forma que son afectados por la Defensa Aérea contra aeronaves convencionales. Dependiendo de la carga táctica que se sospeche, como por ejemplo: armas biológicas, gases químicos o explosivos, puede ser necesario interferir y maniobrar el UAS fuera del alcance de las fuerzas propias o civiles antes de que entre en vigor la contramedida real. Por lo tanto, los enfoques "tradicionales" de C-UAS que surten efecto en el lugar, deben ser revisados y deben considerar nuevos métodos, tales como capturar vehículos aéreos y neutralizar cargas útiles.

CONSIDERACIONES FINALES

Como se describe en este texto, la defensa contra UAS no es solo un problema de Protección de la Fuerza o Defensa Aérea, ni se trata sólo de la aeronave o el dron en sí, y tiene múltiples aristas.

Aun cuando el operador militar natural de los UAS en un Estado es su respectiva Fuerza Aérea, el problema es nacional y de carácter conjunto. Los UAS, no sólo serán empleados por ni contra la Fuerza Aérea. Sin embargo, por cercanía natural con la aviación y con el control del espacio aéreo, la Fuerza Aérea debiera ser la encargada centralizar la planificación y coordinación de la ejecución de las medidas que se decida aplicar.

Las consideraciones legales internacionales e internas, representan un desafío que requiere ser enfrentado desde ahora.

El rápido desarrollo de los sistemas no tripulados o remotamente tripulados, obliga a avanzar en la implementación de políticas, leyes, reglamentos, doctrinas y procedimientos adecuados para enfrentar los tipos de sistemas que aún no representan una amenaza inmediata. Cuando se detecte una amenaza concreta, ya será demasiado tarde.