Sistemas de detección y neutralización de UAVs

Estado del Arte de las Tecnologías

Cátedra Isdefe-UPM

Mayo 2016 – Junio 2017

Madrid, junio de 2017

Introducción

En la actualidad, las tecnologías relacionadas con los vehículos aéreos no tripulados (UAV) están en pleno crecimiento y desarrollo. La cualidad más destacada de este tipo de vehículos es la no necesidad de transportar un piloto a bordo, lo cual resulta atractivo para multitud de aplicaciones tanto civiles como militares.

Centrándonos en los aspectos militares y de seguridad, los UAVs pueden ser utilizados tanto para realizar misiones de reconocimiento enemigo, como para realizar ataques terroristas. Por tanto, el incremento de su uso y la reducción de sus costes conllevan un mayor riesgo de sufrir algún tipo de ataque basado en este tipo de plataformas **[UAV 0.1]**.

Dado que la accesibilidad a los UAVs ha aumentado de forma exponencial en los últimos años, su uso presenta nuevas formas de amenaza, ya sea de forma indirecta porque su mera presencia provoca ciertos riesgos para la población civil, como por ejemplo en los aeropuertos, o de forma directa siendo utilizados en ataques terroristas o en misiones de espionaje. Por este motivo, se ha puesto de manifiesto la necesidad de desarrollar sistemas de protección que hagan frente a estas nuevas amenazas. Prueba del creciente interés de los países miembros de la Unión Europea por el avance de estos sistemas es el programa de trabajo 2016-2017 del Horizonte 2020, que contiene el tema "*Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism*", siendo uno de sus subtemas la detección y neutralización de drones o UAVs ligeros presentes en zonas restringidas **[UAV 0.2]**.

En ámbito de defensa, estos sistemas deben estar basados en el empleo de múltiples tecnologías para conseguir cubrir las capacidades de detección, identificación y neutralización de los UAVs. Sin embargo, estos nuevos tipos de amenazas conllevan retos no completamente resueltos por las tecnologías en el estado del arte, por lo que actualmente constituyen una importante área de investigación.

En la siguiente ilustración se muestra la localización de las principales universidades y centros de investigación, a nivel europeo, relacionados con las tecnologías más novedosas asociadas a la detección, identificación y neutralización de UAV.

Figura 1. Localización de las principales universidades y centros de investigación a nivel europeo (estrellas amarillas).

Tecnologías

Como consecuencia del incremento del uso de los UAV, se ha abierto paso a un nuevo sector referente al desarrollo e investigación de tecnologías ligadas a la detección de estos dispositivos, dando lugar a una activa investigación en diferentes campos de la ingeniería de telecomunicación. La necesidad de los países de protegerse contra las posibles amenazas de este tipo de dispositivos se ha disparado de igual forma que su creciente uso y facilidad de acceso.

Sin embargo, no solo se han desarrollado nuevas técnicas especializadas, sino que algunas son resultado de tecnologías maduras que se afinan para su aplicación en el campo de la detección, la identificación o la neutralización de UAVs.

Además, este sector en desarrollo debe evolucionar continuamente ya que a medida que avanzan las tecnologías para la protección frente amenazas basadas en éstos vehículos, lo hacen de igual forma las defensas que se aplican en los mismos para hacerse invisibles e inmunes.

En lo referente a la protección de infraestructuras críticas se deben cubrir las siguientes capacidades **[UAV 0.3]**:

- Detección del UAV mediante dispositivos de tamaño y coste asumibles. En función del sensor empleado, esta etapa permite obtener distinto tipo de información de los blancos, como su posición angular, distancia al sensor, velocidad o tamaño. Además, es conveniente realizar un seguimiento de los blancos detectados para conocer su trayectoria y generar alarmas tempranas de posibles amenazas. Sin embargo, esta etapa no conlleva diferenciar las detecciones provocadas por UAVs de las de otros blancos que no son de interés como coches o aves.
- Identificación o discriminación del blanco objetivo frente otros objetos o aves que no son de interés y que han sido detectados en la etapa anterior. De esta forma se reduce el número de falsas alarmas y se pueden dirigir los sistemas de neutralización a los UAVs que representen una amenaza.
- Neutralización del UAV en el caso de considerar al mismo como una amenaza, de forma que no lleve a cabo su misión.

Este estudio se centra en la detección, identificación y neutralización de UAVs de clase I, pues dada su disponibilidad en el mercado presentan un mayor interés en el ámbito de defensa,

al constituir una mayor amenaza por la posibilidad de uso indebido de los mismos y por parte de organizaciones terroristas. La Figura 2 muestra varios ejemplos de este tipo de UAVs.

a) b) c)

Figura 2. UAVs de clase I: (a) Nano: Black Hornet, (b) Micro: Phantom 3, (c) Ligero: Hermes 90.

1. Detección

[UAV 1.x.y] es el identificador para las referencias de este apartado, tal como se describe en la sección Anti-UAV del "Documento de Referencias".

En este primer paso el objetivo es conseguir detectar la posición de los blancos alcanzando un compromiso entre la baja sección radar de este tipo de vehículos frente a la detección con aparatos de bajo coste y tamaño reducido. El entorno de aplicación para el que se enfoca cada despliegue tiene un papel decisivo en cuanto a las tecnologías que se utilizan, siendo unas más efectivas que otras.

1.1. Radar convencional

Partimos de la detección UAV mediante la tecnología radar convencional, la tecnología más madura, utilizando radares de onda continua que deben ser compactos y desplegables, por una parte, y de coste asumible. Además, los radares de onda continua, especialmente los de frecuencia modulada, permiten operar en modo LPI (*Low Probability of Interception*), adecuado para aplicaciones en defensa, por su menor potencia de pico y su barrido en frecuencia.

Existen actualmente sistemas radar comerciales optimizados para la detección y seguimiento de UAVs en entornos abiertos como el Drone-Sentinel **[UAV 1.1.1]** que podemos observar en la Figura 3, de la empresa Advanced Radar Technology (ART). Este radar CWLFM (*continuous-wave lineal-frecuency-modulated*) en banda Ku presenta 1 GHz de ancho de banda y 2 W de potencia media transmitida. Además, se están investigando sistemas multiestáticos para mejorar la capacidad de detección de los sistemas radar **[UAV 1.1.2]**.

Figura 3. Drone-Sentinel de ART.

Los retos pendientes que tienen este tipo de radares son debidos a la baja reflectividad de los UAVs **[UAV 1.1.3]**. El pequeño tamaño de los UAV y los materiales de los que están formados, principalmente plásticos, hacen que su sección radar sea pequeña, dificultando así su detección. Además, la capacidad de detección de los radares en banda X o superior puede reducirse en condiciones meteorológicas adversas aunque se ven menos afectados por la lluvia o la niebla que los sensores ópticos.

Por tanto, para detectar y realizar el seguimiento de forma eficaz de este tipo de vehículos es necesario alcanzar un compromiso entre tiempo de iluminación del objetivo y el tiempo de refresco de información.

1.2. Radar persistente

Los radares SIMO (*single-input-multiple-outputs*) y MIMO (*multiple-input-multiple-output*) **[UAV 1.1.4]** tienen la ventaja de ser capaces de cubrir una gran cobertura mediante múltiples haces en acimut y elevación simultáneos en recepción. De esta forma, al no requerir la exploración mecánica o electrónica de los haces, se puede aumentar el tiempo de iluminación e integración sobre los blancos sin afectar al tiempo de refresco de la información por lo que se mejora la capacidad de detección de blancos de sección radar reducida.

Esta arquitectura es capaz de solucionar una parte de los problemas debidos a la baja sección radar de los UAVs y al ocultamiento por el clutter de tierra de los UAVs que vuelan a baja velocidad **[UAV 1.1.5]**.

Sin embargo, el principal problema que presenta este tipo de radares es el aumento de complejidad y tamaño al necesitar al menos tantos receptores y procesadores como distintos haces en acimut y elevación se requieran. Además, se debe evaluar si el aumento del tiempo de integración tiene efectos adversos en la capacidad de detección de UAVs de gran velocidad por la migración en distancia y Doppler que puede producirse. Para mitigar estos efectos, se han desarrollado técnicas de compensación de movimiento, necesarias para blancos veloces y en aceleración **[UAV 1.1.6]**.

1.3. Sonido

La detección de UAVs mediante técnicas acústicas se hace necesaria debido a las limitaciones en la aplicación de las tecnologías radar anteriores. El uso de estos radares es adecuado en entornos abiertos o en infraestructuras aisladas, pero poseen claras limitaciones en entornos urbanos debido al incremento excesivo de detecciones provocadas por otros elementos del entorno, que darían lugar a falsas alarmas.

Algunas soluciones se basan en sensores sísmicos enterrados, creando un perímetro de seguridad en la zona que se desea proteger, con alcances de detección y seguimiento de centenares de metros **[UAV 1.2.7]**. Por otra parte existen sistemas que además son capaces de realizar una clasificación del tipo del UAV y que trabajan con dos tipos de sensores distintos, sensores acústicos omnidireccionales y sensores directivos de largo alcance **[UAV 1.2.8]**.

Otras técnicas tratan la huella digital acústica de los UAV, utilizada también en otros tipos de aplicaciones como en el reconocimiento de canciones **[UAV 1.2.9]** o de personas por el habla **[UAV 1.2.10]**. El objetivo es la identificación de patrones o firmas de un archivo de audio, para que pueda ser reconocido en una base de datos **[UAV 1.2.11]**.

La detección acústica mediante arrays de micrófonos es posiblemente la técnica más prometedora en este tipo de entornos donde los radares no son tan eficaces. El procesado en array permite realizar una estimación de la posición del UAV, aumentar el alcance de detección respecto al uso de un sólo micrófono, y realizar una clasificación basada en su huella sonora **[UAV 1.2.12]**.

Figura 4. Array de micrófonos.

El problema que presenta este tipo de detección es la discriminación y reconocimiento satisfactorio en presencia de otras fuentes de ruido, frente al sonido del UAV. Múltiples investigaciones tratan de mejorar la capacidad de detección de las fuentes sonoras de interés en entornos ruidosos mediante el empleo de arrays de micrófonos y procesados de señal robustos de alta carga computacional **[UAV 1.2.13]**.

Sin embargo, los arrays de micrófonos, al ser sensores pasivos, presentan generalmente un alcance reducido, aunque puede aumentarse o reducirse en función de la dirección del viento. Además, se debe tener en cuenta que los UAVs basados en aeroplanos no pueden ser detectados por esta tecnología al no emitir apenas sonido.

1.4. Vigilancia espectral de radiofrecuencia

Lo que se busca en este caso, es realizar la detección de las señales intercambiadas entre estación base y el UAV mediante equipos de guerra electrónica. Pueden tratarse de comunicaciones UHF, WiFi o por satélite, aunque, en general, los UAVs emplean las bandas de frecuencia de 2,4 GHz, de 5 GHz o de 5,8 GHz **[UAV 1.3.14] ,** en ocasiones de forma simultánea. Una de las opciones para este tipo de detección es mediante la identificación de la modulación utilizada.

Una de las soluciones comerciales disponibles es el sistema Aaronia Drone Detector **[UAV 1.3.15]**, formado por un array de antenas y un analizador de espectros que cubren las frecuencias desde 9 kHz hasta 20 Ghz. El sistema trabaja en tiempo real, capturando y realizando el seguimiento de las emisiones de RF que se producen, activando una alarma automática en el caso de superar los valores máximos. Adicionalmente tiene la ventaja de ser compacto y flexible, dando la opción de desplegarse en pocos minutos en la zona deseada. Gracias al software que incorpora trabajando en tiempo real, se estima la dirección en la que se encuentra el UAV, pudiendo identificar el tipo de UAV y rastrear el operador que lo controla.

Figura 5. Aaronia Drone Detector.

Sin embargo, este método no es capaz de detectar aquellos UAVs “silenciosos” que no mantienen un enlace de comunicaciones con la estación base, sino que están preprogramados para

ejecutar de forma autónoma una misión específica. Por este motivo, en el ámbito de la defensa no es conveniente utilizar sistemas basados únicamente en este tipo de detección.

1.5. Sistemas combinados

En este apartado se trata la posibilidad de sistemas que se basan en la cooperación de las tecnologías que hemos visto anteriormente, trabajando en conjunto para aumentar la efectividad de la detección de los UAVs.

Un ejemplo es la combinación de tecnología radar para realizar la detección de UAVs que se aproximen, estimando la posición del blanco. A continuación se proporciona esta información a un procesador que orienta a los arrays de micrófonos y las cámaras hacia el sector concreto, para realizar una clasificación del UAV o para eliminar falsas alarmas.

Sin embargo, en este tipo de soluciones se debe tener en cuenta la ganancia que realmente aporta añadir la cooperación de una tecnología adicional al sistema, frente al coste tanto económico como de manufactura que conlleva, pues podría no resultar rentable. Además, el uso de múltiples sensores conlleva aumentar el tamaño y los requisitos computacionales del sistema.

2. Identificación

[UAV 2.x.y] es el identificador para las referencias de este apartado, tal como se describe en la sección Anti-UAV del "Documento de Referencias".

La segunda tarea consiste en discriminar los UAV frente a otros objetos o aves con una probabilidad de falsa alarma baja. Esta fase, en la que es necesario realizar de forma satisfactoria la identificación del UAV frente a otras posibilidades, juega un papel clave, ya que sobre ella recae la responsabilidad de determinar si el objeto que se aproxima representa una amenaza antes de pasar al siguiente paso de neutralización.

Para reducir el número de falsas alarmas se requiere una rápida clasificación del blanco, mediante reconocimiento automático o con un operador convencional que revise la información, antes de realizar el seguimiento del mismo y, en caso de necesidad neutralizar al objetivo.

La posibilidad de la identificación automática, sin necesidad de un operador que revise la información recogida, es el principal reto tecnológico de esta fase.

2.1. Microdoppler

Una de las técnicas que está en pleno desarrollo es la identificación mediante la firma microdoppler de los UAV mediante sistemas radar. El crecimiento del uso de UAV de tamaño "mini" de características de baja altitud, sección radar pequeña y baja velocidad hacen que la clasificación y discriminación de aves frente a ellos presente un reto **[UAV 2.1.16]** ya que presentan similitudes en su sección radar y en los patrones de vuelo **[UAV 2.1.17]**.

La firma microdoppler de un objeto depende tanto del movimiento y rotación de las piezas, como del movimiento del cuerpo principal del mismo. Es una técnica que permite diferenciar UAVs de aves y da la posibilidad de realizar una clasificación de distintos tipos de UAV, estimando el tamaño y el número de rotores que posea **[UAV 2.1.18]**.

Se han realizado números experimentos trabajando con ésta técnica y todos son capaces de realizar discriminaciones satisfactorias frente aves, además de ser capaces de clasificar el tipo de UAV, consiguiendo realizar un reconocimiento automático de los blancos**[UAV 2.1.19]**.

2.2. Imagen

La identificación de UAVs mediante técnicas de cámaras de infrarrojos e hiperespectrales es un campo en el que se está trabajando activamente en la actualidad. Éstas técnicas abarcan desde sistemas que trabajan en el espectro visible, cámaras que trabajan en el infrarrojo hasta nuevos sistemas que buscan trabajar en todo el espectro mediante cámaras hiperespectrales. Esta tecnología se basa en realizar el procesado de las imágenes capturadas para identificar los UAVs y diferenciarlos de otros objetos automáticamente.

Como se puede observar en la Figura 6, la identificación mediante sistemas pasivos que trabajan el infrarrojo se basan en cámaras que detectan la huella de calor del UAV. Tienen la capacidad de trabajar en oscuridad sin emitir potencia por lo cual es una ventaja para su aplicación en el campo de la defensa ya que estos sensores no pueden ser detectados por equipos de guerra electrónica. Aunque pueden operar en condiciones meteorológicas adversas como niebla o lluvia **[UAV 2.2.20]**, su correcto desempeño se ve más afectado que el de los sistemas radar.

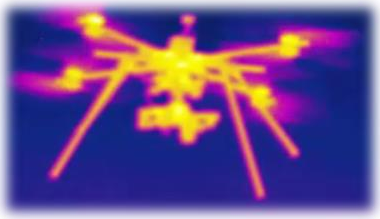

Figura 6. Imagen infrarroja de un UAV.

Por otra parte, la identificación mediante cámaras hiperespectrales **[UAV 2.2.21]** da la posibilidad de cubrir todo el espectro electromagnético, lo que representa una ventaja respecto a las cámaras vistas anteriormente para mejorar la capacidad de identificación de los objetos. Actualmente tienen el problema de que conllevan una carga de proceso grande **[UAV 2.2.22]**. Sin embargo, pese a no ser actualmente una tecnología madura, tiene muchas posibilidades de cara al futuro, en la identificación automática de blancos, sin necesidad de un operador adicional que revise la información obtenida.

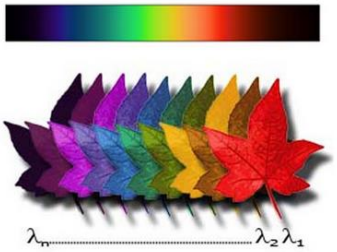

Figura 7. Imagen hiperespectral.

2.3. Identificación de amenaza

En este caso, se da un paso más en lo referente a la identificación del UAV, pues una vez realizada la tarea de reconocer al objetivo como un UAV frente a otras posibilidades, se debe analizar si el mismo transporta algún tipo de carga peligrosa, por ejemplo explosivos y armas químicas o bacteriológicas.

Para realizar este cometido, operadores convencionales se encargan de revisar en la medida de lo posible la carga que portan éstos vehículos a partir de las imágenes obtenidas, aunque se han realizado avances recientes en los que se emplea otro UAV, como el SpectroDrone, que podemos observar en la Figura 8, encargado de la misión de analizar la carga del UAV considerado como amenaza utilizando tecnología láser **[UAV 2.3.23]**.

Figura 8. SpectoDrone.

2.4. Deteccion de emisiones RF

Este metodo de deteccion, se basa en que la mayoria de los RPAS poseen multiples sistemas de comunicaciones. Dichos sistemas al establecer una comunicacion dejan una huella en el espectro radiolectrico que puede ser detectada. Estos detectores barren el espectro con una o varias antenas buscando sistemas de comunicaciones que utilizan los drones habitualmente. Dependiendo de la complejidad del sistema, este puede permitir locaclizar la ubicacion desde la que se originan las comunicaciones y por lo tanto al operador del drone. Un ejemplo de este tipo de sistemas es Drone Alert (Rohde & Schwartz) que se puede ver en la siguiente figura.

Figura 9 Drone Alert. Rohde & Schwartz

3. Neutralización

[UAV 3.x.y] es el identificador para las referencias de este apartado, tal como se describe en la sección Anti-UAV del "Documento de Referencias".

Una vez realizado el proceso de detección e identificación, si consideramos que el UAV representa una amenaza, debemos llevar a cabo alguna técnica de anulación. A medida que la industria de los UAV evoluciona, también lo hacen las prestaciones de los mismos en lo referente a sus capacidades de defensa propias, por lo tanto, el sector de tecnologías asociadas a la neutralización debe estar preparado para las novedades de los UAV más modernos.

El tipo de tecnologías de neutralización a emplear tiene una alta dependencia con el entorno en el que se desee instalar el sistema, siendo unas técnicas más apropiadas que otras. La presencia o ausencia de población civil representa uno de los parámetros a tener en cuenta en la elección del sistema adecuado, evitando poner en riesgo la seguridad de las personas.

3.1. Métodos basados en interferencias

3.1.1. GPS spoofing

La mayoría de los UAVs están equipados de receptores GPS para realizar distintas misiones de navegación y guiado. El GPS spoofing consiste en intentar "engañar" al UAV, es decir, transmitirle señales GPS falsas para que el vehículo crea que está en otro lugar distinto del que realmente está, apoderándose del control del mismo **[UAV 3.1.24]**.

Se han realizado numerosos estudios sobre las vulnerabilidades del GPS, y en consecuencia se han desarrollado multitud de sistemas comerciales basados en ésta técnica, tanto dispositivos fijos como desplegables, ejemplos de ello se muestran en la Figura 10 **[UAV 3.1.25] [UAV 3.1.26]**.

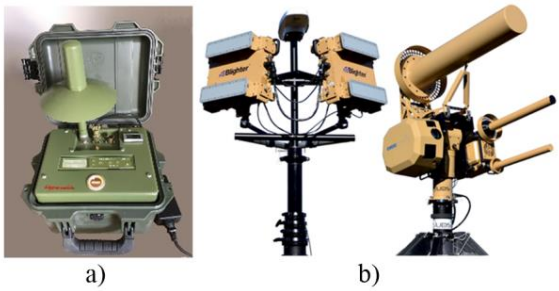

Figura 10. Sistemas con GPS spoofing: a) ClearSky, b) Blighter AUDS.

Uno de los problemas actuales, es que los UAV más sofisticados están equipándose con sistemas en los que la navegación y guiado no dependen del uso del GPS sino que utilizan sistemas inerciales para navegar de forma autónoma, por lo tanto se deben buscar nuevas soluciones. Adicionalmente, el uso de la técnica GPS spoofing no está permitido en todos los países como EE. UU. **[UAV 3.1.27]**, por lo que se deben valorar también otras alternativas.

3.1.2. Jamming

A diferencia de la técnica anterior, las tecnologías jamming no tiene como fin apoderarse del UAV, únicamente busca crear interferencias para que éste no funcione correctamente o cortar el enlace de comunicaciones con su estación base.

El uso de ésta técnica debe ser controlado, ya que no se sabe con certeza cómo reaccionará el UAV, pudiendo provocar amenazas si lleva cargas peligrosas como armas explosivas o químicas o si hay presencia de población civil en sus alrededores, por tanto su uso no es conveniente en cualquier tipo de entorno.

De la misma forma que en el apartado anterior, se han desarrollado sistemas tanto fijos como desplegables, como las "pistolas jammer", tal y como se observa en la Figura 11, son utilizadas por un operador convencional apuntándolas hacia el UAV que representa una amenaza**.**

Figura 11. Batelle DroneDefender.

3.1.3. Hacking de las comunicaciones WiFi

Uno de los tipos de comunicaciones que pueden establecerse entre estación base y el UAV es mediante una conexión WiFi. De esta forma, se pueden realizar varios tipos de ataques sobre esta conexión para interrumpir las comunicaciones.

Los sistemas transmisores y receptores tienen que saber a quién deben transmitir y escuchar, por tanto se produce un intercambio de tramas al comienzo de la comunicación para asociar los dispositivos. En muchas ocasiones esta parte del proceso no está protegida, lo que causa vulnerabilidades a la hora de recibir un posible ataque.

3.2. Métodos de anulación física

3.2.1. Láser

Se han desarrollado armas basadas en tecnología láser de alta potencia que consiguen derribar a los UAV a una distancia de hasta 1 km enfocando de forma precisa el haz láser hacia la posición del drone. Estos sistemas requieren el empleo de sensores, como radares o cámaras, que permitan identificar la amenaza y localizarla de forma muy precisa realizando un seguimiento de la misma antes de derribarla.

Las principales desventajas de estos sistemas son su elevado coste y peso, aunque actualmente se están desarrollando sistemas más compactos. Además, se deben tener en cuenta los aspectos de seguridad y los permisos necesarios para el empleo de este tipo de armas además de las limitaciones impuestas por la convención de Ginebra en su protocolo IV que limita el uso de armas láser. Sin embargo, dada la elevada precisión y enfoque de energía en estos sistemas, se ha demostrado que el empleo de armas láser permite neutralizar los drones con menores daños colaterales e impacto en el entorno que utilizando otros tipos de armas como proyectiles o armas de fuego. Su capacidad de ataque incremental y el uso de munición no explosiva son otras de sus ventajas.

Existen varios tipos de sistemas láser en función de las técnicas que se utilizan para generar el haz. Estas categorías son:

- High-power diode laser arrays: Estos sistemas están formados por pilas de diodos laser individuales o multistripe. Su gran ventaja es su gran eficiencia electro-óptica, aunque presentan una baja calidad de haz. Su máxima eficiencia se alcanza en longitudes de onda comprendidas entre 880nm y 980nm, aunque pueden funcionar entre 400nm y 2200nm. Alcanzan potencias de hasta 1kW utilizando refrigeración activa.

- High-power solid-state lasers: Un láser de estado sólido es un láser que utiliza un medio de ganancia que es un sólido. Generalmente consiste en un material de vidrio al que se añade un "dopante"(neodimio, cromo, erbio, tulio o iterbio). Mediante esta técnica se pueden conseguir eficiencias de hasta 60% y potencias de salida de hasta 30kW.

- Optical fiber lasers: Estos sistemas generan el haz utilizando fibra óptica de núcleo dopado. Utilizando esta técnica se pueden alcanzar eficiencias de hasta 46% y potencias inferiores a 1kW.

- Beam combining: El beam combining no es una técnica de generación en sí, sino que es una forma de superar las limitaciones de potencia de los diferentes sistemas mediante combinaciones de haz. Hay 3 modos de combinación:

    - Combinación coherente. Utilización de interferencia constructiva.

    - Wavelength combining. Combinación de varias longitudes de onda en un solo haz mediante redes de difracción o espejos dicroicos.

- Hibrida. Consiste en la utilización de las dos técnicas anteriores de manera simultánea.

- Heat-capacity lasers. Son sistemas de estado sólido que utilizan diferentes técnicas para aumentar la potencia de salida. Alcanzan hasta los 67kW. Esto se consigue agregando rápidamente disparos individuales haciendo que el calor residual se almacene en el medio. La no utilización de medios de refrigeración permite menos distorsiones ópticas en el sistema y por tanto mayor potencia de salida del láser.

- Chemical lasers. La energía y el haz se obtienen mediante reacciones químicas, y el sistema se refrigera mediante el flujo de gases. Se pueden alcanzar potencias del orden de 100kW en frecuencias cercanas a los infrarrojos.

Estas técnicas se han implementado en diferentes sistemas de defensa que ya están en el mercado o que se espera que estén disponibles en los próximos años. Algunos ejemplos de estos sistemas son:

Nombre del sistema	Fabricante	Tipo	Características	Estado de desarrollo
LaWS [UAV 3.2.55]	Kratos	Solid State	30kW. Embarcado.	En uso. USS Ponce
Oerlikon [UAV 3.2.30]	Rheinmetall	Fibra & Beam Combining	10kW. Ground based.	En el mercado.
Silent strike [UAV 3.2.31]	Boeing		10kW. 22 millas de alcanza. Desmontable y ligero	En el mercado.
Iron Beam [UAV 3.2.56]	Rafael		Sin información publica	En el mercado.
Lockheed Martin Laser System [UAV 3.2.57]	Lockheed Martin	Solid state & Beam Combining	60kW	En desarrollo.
Hellads [UAV 3.2.58]	Darpa & Weaponer Textron	Combinación de láseres químicos y de estado sólido.	150kW. Pequeño tamaño	En desarrollo. 2020
Excalibur [UAV 3.2.59]	Darpa	Beam combining	Orden de kW para cada laser.	En desarrollo. 2020.

Debido a que el desarrollo de los sistemas láser está en auge, están surgiendo a su vez sistemas de defensa contra ellos. A continuación, listamos algunos de ellos:

- Sistemas basados en "espejos”

- Materiales ablativos: Absorben la energía del láser y generan gas.

- Thermal transport delay. Ralentización de la propagación del calor mediante capas de materiales aislantes.

- Obscurants and atmospheric degradation. Generar polvo o humo para reducir la efectividad.

- Meta materiales. Ttodavía en etapas tempranas de desarrollo.

- Preyecto Helios. Sistema de senseres para descubrir el laser y laser propio para apuntar al laser atacante y confundirlo haciéndole creer que no está enfocado.

3.2.2. Redes

Existen métodos comerciales desarrollados mediante los cuales un único operador con un sistema transportable dispara un proyectil que es capaz de alcanzar al UAV, atrapándolo con una red o derribándolo. En algunos sistemas en los que se lanza una red, el UAV cae de forma segura gracias a un paracaídas sin sufrir daños **[UAV 3.2.32]**

En el siguiente caso, un UAV (dron anti-dron) vigila el perímetro mediante una cámara de alta resolución. En el caso de que un UAV sea detectado e identificado como amenaza por parte de los sistemas anteriormente expuestos o por el propio dron anti-dron, éste lanzará una red para inmovilizar a la amenaza, como se muestra en la Figura 12, dejándolo caer mediante un paracaídas o llevándolo a un lugar seguro **[UAV 3.2.33] [UAV 3.2.34].**

Figura 12. Anti-dron Excipio.

Éstas técnicas, que están en desarrollo, podrían ser útiles en entornos donde no conviene utilizar contramedidas electrónicas y en los que se debe controlar el punto de caída del UAV que representa una amenaza.

3.2.3. Águilas

El entrenamiento de águilas para la caza de UAVs es una práctica que se está realizando en varios países. Los UAVs son identificados como una presa para las águilas, para después dejarlos en un lugar seguro **[UAV 3.2.35].**