ieee.es
Instituto Español de Estudios Estratégicos

Documento
Marco

21/2018 29 de noviembre de 2018

*José Alberto Marín Delgado**

El sistema de defensa aérea no-cinético, clave para la defensa antidrón

El sistema de defensa aérea no-cinético, clave para la defensa antidrón

Resumen

Los sistemas de defensa aérea tradicionales basan sus capacidades de neutralización, por norma general, en sistemas de armas cinéticos. Se basan en una concepción tradicional frente a un enemigo convencional. La aparición de los drones ha supuesto un cambio de paradigma para la defensa aérea. Esta nueva amenaza es furtiva, económica, numerosa, tecnológicamente avanzada y flexible, características que suponen un verdadero hándicap para los sistemas de armas cinéticos. Los sistemas de armas no-cinéticos cubren muchas de las limitaciones de los sistemas de armas cinéticos, por lo que son un complemento para una defensa aérea eficiente frente a la amenaza dron.

Palabras clave

Dron, defensa aérea, C-UAS, no-cinético, láser, HPM, DEW, ciberdefensa.

The non-kinetic air defense system is key to anti-drone defense

Abstract

The traditional air defense system bases their neutralization capacities, generally speaking, on kinetic weapons systems. They are based on the traditional conception against a traditional enemy. However, with the arising of drones, a new scenario has emerged regarding air defense. The new threat is furtive, economical and large; technologically speaking is advanced and flexible. All these characteristics together lead to a real disadvantage for the kinetic weapons systems. The non-kinetic weapons systems fill the gaps of the kinetic weapons system; therefore they are a successful complement towards an efficient air defense in order to handle the drone threat.

Keywords

Drone, Air Defense, C-UAS, non-kinetic, Laser, HPM, DEW, cyberdefense.

¿Cuál es la idea fundamental de la defensa?
Es la de parar un golpe.
¿Por qué señal se distingue?
Se distingue porque en ella se espera el golpe que se debe parar.
Carl von Clausewitz.

Introducción

La estructura tradicional de los sistemas de defensa aérea (SDA)[1] se basa en una combinación de medios para la detección e identificación de amenazas aéreas y el empleo de medios cinéticos, aéreos o basados en superficie, para su neutralización. Todo ello articulado bajo los principios de mando centralizado, ejecución descentralizada y defensa en profundidad.

Esta concepción está basada en un desarrollo doctrinal post-Guerra Fría, en la cual los sistemas de defensa aérea debían enfrentarse a tres amenazas principales[2]:

- Aeronaves hostiles.
- Misiles Balísticos.
- Misiles de crucero.

Esta concepción doctrinal ha sido efectiva hasta la aparición de un nuevo paradigma, los vehículos aéreos no tripulados (VANT), también conocidos como drones[3].

Los drones como amenaza para el espacio aéreo

La explotación del dominio aéreo en el campo de batalla, desde la aparición de los primeros artefactos voladores, ha estado reservada a actores estatales debido a sus especiales características y necesidades. La instrucción general (IG) 00-01 sobre Doctrina Aeroespacial del Ejército del Aire, enumera una serie de factores condicionantes que afectan al Poder Aeroespacial como son su elevado coste, su sensibilidad a la tecnología, su detectabilidad y su dependencia de bases, entre otros. Los drones han superado varios de los factores condicionantes siendo gran número de ellos no dependientes de bases, con una detectabilidad en multitud de casos similar a la

[1] En inglés *air defense system* (ADS).
[2] EVAN, R. C., «National Air Defense: Challenges, Solution Profiles, and Technology Needs», The MITRE Corporation, USA.
[3] En este documento se utilizarán términos como dron, VANT, UAS (*unmanned aerial system*), UAV (*unmanned aerial vehicle*) o RPA (*remotely piloted aircraft*) para referirse a los vehículos aéreos no tripulados o a sus sistemas.

de aviones furtivos[4], tecnológicamente avanzados favorecidos por una revolución en campos como la computación y la robótica, todo ello a un coste muy reducido frente a sistemas aéreos tradicionales. Todos estos factores han permitido que actores con medios muy limitados, tanto estatales como no-estatales, accedan a la explotación del espacio aéreo, multiplicándose el número de usuarios y aumentado de manera exponencial el número de artefactos en el dominio aéreo. En definitiva, los drones aéreos suponen lo que se conoce en la doctrina anglosajona como un *game-changing*, es decir, un instrumento innovador que está revolucionando la forma de hacer la guerra.

El Departamento de Defensa de Estados Unidos clasifica los drones en 5 grupos basados en su peso, altitud y velocidad de operación. Los drones pertenecientes a los grupos 1, 2 y 3 son conocidos como LSS UAS[5], que vienen a ser drones de pequeño tamaño que operan a baja altitud y velocidad[6].

La clasificación de la tabla 1, basada en peso, altura y velocidad ha quedado obsoleta, puesto que hay drones del grupo 1 con techos de vuelo del grupo 5, por lo que se deberían estudiar nuevas clasificaciones basadas en otros parámetros (nota del autor).

[4] Para más información RAA número 875. Artículo «Drones, la nueva amenaza para el espacio aéreo» pp. 530-531. http://www.ejercitodelaire.mde.es/EA/ejercitodelaire/es/.galleries/anexos/revista/RAA-Julio-Agosto.pdf

[5] Del inglés *low-slow.small unmanned aircraft system*.

[6] ATP 3-01.81.

Grupo	Peso máximo al despegue (Libras)	Altitud de Operación Normal (Pies)	Velocidad (Nudos)	Observaciones
1	0 - 20	< 1200 AGL	100	Normalmente lanzados manualmente.
2	21 - 55	< 3500 AGL	< 250	Sistemas pequeños con reducida RCS[7] y autonomía media.
3	< 1320	< FL 180		Alcance y autonomía significativos. Requieren logística superior a los anteriores
4	> 1320		Cualquier velocidad	De tamaño considerable, operan a altitudes medias-altas. Alcance y autonomía extendida. Por norma general requieren pistas para su operación
5		> FL 180		Operan entre media y alta altitud. Necesidades logísticas similares a una aeronave tripulada

Tabla 1: Clasificación UAS. Fuente: ATP 3-01.81

Los drones de los grupos 4 y 5 suponen una amenaza semejante a la de las aeronaves tripuladas, puesto que su ámbito de operación es similar en términos de altitud, detectabilidad (RCS), necesidades logísticas, o incluso precio en muchos casos, por lo que este tipo de amenaza se podría llegar a acometer de igual forma que una amenaza convencional. Este tipo de aeronaves, debido a sus necesidades logísticas y tamaño, tienen una trazabilidad relativamente sencilla a diferencia del resto de grupos.

En cuanto a los grupos 1, 2 y 3 o LSS UAS, suponen un verdadero hándicap para los SDA, debido a sus especiales características los procesos de detección, identificación y neutralización son sumamente complejos y difícilmente «acometibles» por los sistemas de armas actuales, como se desarrollará con posterioridad.

Independientemente de la clasificación de los drones y su tipología, para que resulten una amenaza para los SDA, su presencia en número debe ser significativa. Según varios informes del *Global Market Insights*, el mercado de drones militares se estimaba en 2016 en aproximadamente 5.000 millones de dólares con una flota estimada de 13.000 unidades y un crecimiento anual de aproximadamente el 12 %. A su vez el mercado de

[7] Del inglés *radar cross section*. Es una medida que indica la capacidad de un objeto de ser detectado por un RADAR. A mayor RCS mayor probabilidad de ser detectado.

drones de entre 25 y 150 kilogramos (grupos 2 y 3) supondrá un 50 % del total hasta 2024 y el crecimiento en el mercado de drones de más de 150 kilogramos se estima en un 11 % anual[8]. En cuanto al mercado civil de drones[9], a considerar debido al posible uso ilícito de estos sistemas, las estadísticas son más dramáticas. El mercado de drones de uso recreativo en 2016 se cifraba en más de 2 millones de unidades, con un crecimiento anual estimado de 18 % hasta 2024[10]. Por otro lado el mercado de drones para aplicaciones comerciales en 2016 se estimaba en torno a 100.000 unidades con un crecimiento anual estimado de 25 % hasta 2024[11]. Estas cifras indican el crecimiento sin precedentes de estos artefactos aéreos y la previsible saturación del dominio aéreo.

Limitaciones de los SDA basados en sistemas de armas cinéticos frente a drones

Los Sistemas de Defensa Aérea actuales emplean mayoritariamente sistemas de armas cinéticos para neutralizar amenazas aéreas. Como vimos anteriormente, se basan en una concepción de defensa en profundidad, frente a una amenaza convencional. A su vez esta concepción estaba basada en un principio de superioridad ante un posible enemigo o en caso contrario en una acumulación de fuerzas tal que, aun siendo inferiores a un posible enemigo, el nivel de atrición que sufriría, disuadiría a este de realizar tal acción.

Los sistemas de armas cinéticos son totalmente válidos para amenazas convencionales así como para drones de los grupos 4 y 5, debido a su similitud a las aeronaves tripuladas, como se indicó anteriormente. Pero su utilización frente a drones de los grupos 1, 2 y 3 o LSS UAS presenta una serie de limitaciones que deben ser evaluadas. Entre estas limitaciones podemos destacar:

[8] https://www.gminsights.com/industry-analysis/military-drone-market.
[9] Se han utilizado en multitud de ocasiones drones civiles en acciones ilícitas de diversa índole. El grupo terrorista ISIS es un ejemplo de usuario de drones civiles en acciones militares. Para más información: http://www.ieee.es/Galerias/fichero/docs_marco/2018/DIEEEM03-2018_DronesComerciales-VectoresTerroristas_JAMarinDelgado.pdf
[10] https://www.gminsights.com/industry-analysis/consumer-drone-market.
[11] https://www.gminsights.com/industry-analysis/unmanned-aerial-vehicles-UAV-commercial-drone-market.

Daño colateral

Una de las características principales de los LSS UAS es que la gran mayoría de estos sistemas son de reducido tamaño, por lo que pueden ser transportados fácilmente, incluso en una mochila y su operación requiere de unas necesidades logísticas mínimas. Por otro lado estos sistemas son multiplicadores de la fuerza en combates urbanos, por lo que su uso en este entorno se está generalizando. La neutralización de LSS UAS 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.

Por ejemplo, en julio de 2016 las Fuerzas de Defensa de Israel (IDF[12]) dispararon dos misiles *Patriot* contra un dron de la organización terrorista Hezbolá que penetró en espacio aéreo israelí. Los misiles no hicieron blanco y sus restos hirieron a una niña de 14 años[13,14].

Una de las ventajas de los sistemas de armas no cinéticos, como se verá con posterioridad, es que multitud de estos son capaces de neutralizar amenazas aéreas sin recurrir a su destrucción o, en caso de producirse, se realiza por medio de energía electromagnética, con la consiguiente ventaja que supone para minimizar el daño colateral.

Economía

Como se comentó anteriormente, uno de los éxitos de la proliferación de los drones y en concreto de los LSS UAS es su reducido coste frente a otros sistemas aéreos convencionales. Los SDA basados en armamento cinético asumen unos costes de empleo frente a un enemigo convencional relativamente equilibrados y en muchos casos beneficiosos, por lo que su operación es asumible y justificable por un ejército. Por ejemplo, el empleo de un misil antiaéreo tipo *Patriot PAC-3 MSE*, con un costo estimado de entre 4,7 y 5,6 millones de dólares[15] frente a un aeronave tipo caza F-16 C/D Block 50/52 con un coste estimado de 18,8 millones de dólares[16] es totalmente asumible y

[12] Del inglés *Israel Defense Forces*.
[13] https://www.pressreader.com/israel/the-jerusalem-post/20160718/281505045563627
[14] El misil Patriot PAC-2 mide 5,8 metros y pesa en torno a 900 kilos https://www.armyrecognition.com/united_states_american_missile_system_vehicle_uk/patriot_mim-104_surface-to-air_defense_missile_data_sheet_specifications_information_description.html
[15] Selected Acquisition Report (SAR),«Patriot Advanced Capability-3 Missile Segment Enhancement (PAC-3 MSE)», March 2016, disponible en http://www.dtic.mil/dtic/tr/fulltext/u2/1019515.pdf
[16] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104505/f-16-fighting-falcon/

favorable en costos económicos. Pero el empleo de ese mismo misil frente a un dron tipo LSS UAS será en multitud de casos inaceptable e insostenible[17].

SISTEMA	PRECIO ESTIMADO (dólares)
F-100 / MISIL SM-2 MR	1,7-1,8 millones[18]
PATRIOT / MISIL PAC-3 MSE	4,7-5,6 millones[19]
NASAMS / MISIL AIM-120 C	300.000 – 400.000[20]
HAWK / MISIL MIM-23 HAWK	250.000[21]
MISIL MISTRAL	120.000[22]
MISIL IRIS-T	455.000[23]
CAÑÓN OERLIKON 35 / MUNICIÓN 35 mm AHEAD[24]	1.000 – 1786[25] 1.786 x 25 disparos (ráfaga)[26] 44.650

Tabla 2. Precio estimado de diferentes sistemas de armas cinéticos
Elaborada por el autor

[17] Según el general David Perkins, comandante del *Training and Doctrine Command* (TRADOC) del ejército americano, en una ponencia en el AUSA *Annual Meeting* en marzo de 2017, afirmó que un aliado de Estados Unidos derribó un dron comercial de 200 dólares con un misil *Patriot* de 3.4 millones de dólares. El general recalcó la grave dificultad económica que supone y la necesidad de reconocer la naturaleza del problema y presentar nuevas y más apropiadas respuestas a esta amenaza. Para más información: https://www.youtube.com/watch?v=6v7nfB5bV3E.

[18] http://nation-creation.wikia.com/wiki/Modern_Day_Military_Pricing_List

[19] «Patriot Advanced Capability-3 Missile Segment Enhancement (PAC-3 MSE)», Selected Acquisition Report (SAR), March 2016, disponible en http://www.dtic.mil/dtic/tr/fulltext/u2/1019515.pdf

[20] Precio estimado diversas fuentes.

[21] Precio estimado diversas fuentes.

[22] https://elpais.com/diario/1991/12/14/espana/692665225_850215.html

[23] https://web.archive.org/web/20131024113307/http://www.revistatenea.es/revistaatenea/revista/PDF/documentos/Documento_1026.pdf.

[24] Del inglés *advanced hit efficiency and destruction.* Para más información sobre esta munición: https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2005/garm/tuesday/buckley.pdf

[25] http://www.pmulcahy.com/ammunition/autocannon_ammunition.html

[26] Para asegurar la letalidad de esta munición diversas publicaciones y fabricantes sugieren disparos de ráfagas de 25 proyectiles para generar una nube de submuniciones y aumentar la probabilidad de derribo. Más información: https://defense-update.com/20040221_ahead.html o https://www.forecastinternational.com/archive/disp_pdf.cfm?DACH_RECNO=816.

DRON	PRECIO ESTIMADO (dólares)
MQ-9 REAPER	< 20 millones[27]
SEARCHER MK III	5,3 millones[28]
PHANTOM 4 PRO V2.0	1.499[29]
X8 LONG RANGE	1.999[30]

Tabla 3. Precio estimado de diferentes tipos de drones
Elaborada por el autor

Realizando una comparativa entre los sistemas de armas de la tabla 2 y los drones de la tabla 3 se puede identificar que el empleo de los sistemas de armas cinéticos frente al dron MQ-9 (categoría 5) es ventajoso en términos económicos, así como en el caso del SEARCHER (categoría 3). Por otro lado para los drones PHANTOM y X8 (categoría 1) con excepción de la neutralización por medio de cañón, el empleo del resto de sistemas de armas cinéticos, en términos económicos, es desorbitadamente deficitario[31].

---

[27] Precio estimado por unidad del contrato de venta realizada al Ejército del Aire de España. Fuente *S*[27]*???* Según el general David Perkins, Comandante del *Training and Doctrine Command* (TRADOC) del ejército americano, en una ponencia en el AUSA *Annual Meeting,* en marzo de 2017, afirmó que un aliado de Estados Unidos derribó un dron comercial de 200 dólares con un misil *Patriot* de 3.4 millones de dólares. El general recalcó la grave dificultad económica que supone y la necesidad de reconocer la naturaleza del problema y presentar nuevas y más apropiadas respuestas a esta amenaza. Para más información: https://www.youtube.com/watch?v=6v7nfB5bV3E.

[27] http://nation-creation.wikia.com/wiki/Modern_Day_Military_Pricing_List

[27] «Patriot Advanced Capability-3 Missile Segment Enhancement (PAC-3 MSE)», Selected Acquisition Report (SAR), March 2016, disponible en http://www.dtic.mil/dtic/tr/fulltext/u2/1019515.pdf

[27] Precio estimado diversas fuentes.OJO REVISAR ESTAS NOTAS CON MISMA NUMERACIÓN

[27] Precio estimado diversas fuentes.PERTENECE TODO A LA NOTA 27?

[27] https://elpais.com/diario/1991/12/14/espana/692665225_850215.html

[27] https://web.archive.org/web/20131024113307/http://www.revistatenea.es/revistaatenea/revista/PDF/documentos/Documento_1026.pdf.

[27] Del inglés *advanced hit efficiency and destruction.* Para más información sobre esta munición: https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2005/garm/tuesday/buckley.pdf

[27] http://www.pmulcahy.com/ammunition/autocannon_ammunition.html

[27] Para asegurar la letalidad de esta munición diversas publicaciones y fabricantes sugieren disparos de ráfagas de 25 proyectiles para generar una nube de submuniciones y aumentar la probabilidad de derribo. Más información: https://defense-update.com/20040221_ahead.html o https://www.forecastinternational.com/archive/disp_pdf.cfm?DACH_RECNO=816.

[27] Precio estimado por unidad del contrato de venta realizada al Ejército del Aire de España. Fuente *ecurity Cooperation Agency*. http://www.dsca.mil/sites/default/files/mas/spain_15-54.pdf

[28] https://www.infodefensa.com/es/2009/09/08/noticia-espana-compra-a-eads-e-indra-un-nuevo-uav-por-53-millones-de-euros.html

[29] https://store.dji.com/product/phantom-4-pro-v2?vid=43151

[30] https://www.uavsystemsinternational.com/product/x8-long-range-drone/

[31] El grupo terrorista ISIS ha utilizado drones comerciales modificados tipo PHANTOM y X8 para realizar acciones ofensivas. Para más información: http://www.ieee.es/Galerias/fichero/docs_marco/2018/DIEEEM03-2018_DronesComerciales-VectoresTerroristas_JAMarinDelgado.pdf

La economía en la guerra es vital y puede ser determinante en el éxito de una contienda. Como dijo Napoleón Bonaparte «Para hacer la guerra se necesitan tres cosas: dinero, dinero y dinero».

Cantidad

Este concepto está íntimamente relacionado con el anterior ya que, a mayor poder económico, mayor cantidad de sistemas de armas se pueden adquirir. La doctrina tradicional sobre la que se basan los SDA actuales, como se vio anteriormente, delimita las amenazas aéreas en tres tipos[32]. Estas amenazas debido a su elevado coste, sus necesidades logísticas en muchas de ellas o su tamaño, permiten realizar sobre las mismas una trazabilidad, de tal manera que se pueden articular las defensas propias en función de las capacidades del enemigo o, por otro lado, se puede restringir la adquisición de diferentes sistemas por medio de tratados de no proliferación como el *Missile Technology Control Regime* (MTCR)[33]. A su vez, el elevado coste en la gran mayoría de las mismas justifica la adquisición de un número determinado de sistemas cinéticos para contrarrestar esta amenaza. Es por ello que se aboga por un equilibrio de fuerzas basado en unas cantidades que puedan hacer frente a una hipotética amenaza. Los drones y su reducido coste frente a aeronaves tripuladas han permitido elevar exponencialmente el número de actores aéreos, provocando un desequilibrio en los SDA actuales. Este desequilibrio no es solo económico como vimos anteriormente, sino también de material. Actualmente ningún sistema de armas cinético puede hacer frente a un ataque masivo de drones y, en el caso de que pudiera hacerle frente, el coste económico y de material sería inasumible. Por otro lado, no hay que olvidar que la amenaza convencional no solo sigue presente, sino que cada vez es más efectiva y letal, por lo que no puede descartarse.

Los ataques por saturación son unos de los escenarios más complejos a enfrentar por los SDA. Este tipo de ataque con drones, además de su ventaja en términos económicos frente a sistemas tripulados, destaca que, al desaparecer el componente humano, sus acciones pueden ser suicidas, desapareciendo los criterios de cumplimiento de nivel de riesgo para aeronaves tripuladas[34], aumentando enormemente su letalidad.

[32] Se enumeran en el apartado Introducción.
[33] Más información: http://mtcr.info/
[34] En la doctrina occidental existen tres niveles de riesgo para las acciones aéreas, nivel de riesgo bajo, medio y alto. Cada nivel indica un grado de riesgo a cumplir por las tripulaciones en función de los objetivos

Los ataques por saturación se van a ver favorecidos por el desarrollo de la tecnología de enjambre de drones o *swarm*[35]. Esta tecnología permite a los drones no solo operar de forma autónoma, sino que también de forma cooperativa y adaptativa al entorno. Estos desarrollos permitirán a su vez acciones de minado aéreo, pudiendo negar parte del espacio aéreo. Ejemplos de esta tecnología son el programa Gremlin de la agencia DARPA[36] o los drones Perdix, desarrollados por el Instituto de Tecnología de Massachusetts (MIT), probados satisfactoriamente en una misión colaborativa de 103 artefactos lanzados desde cazas F/A-18[37].

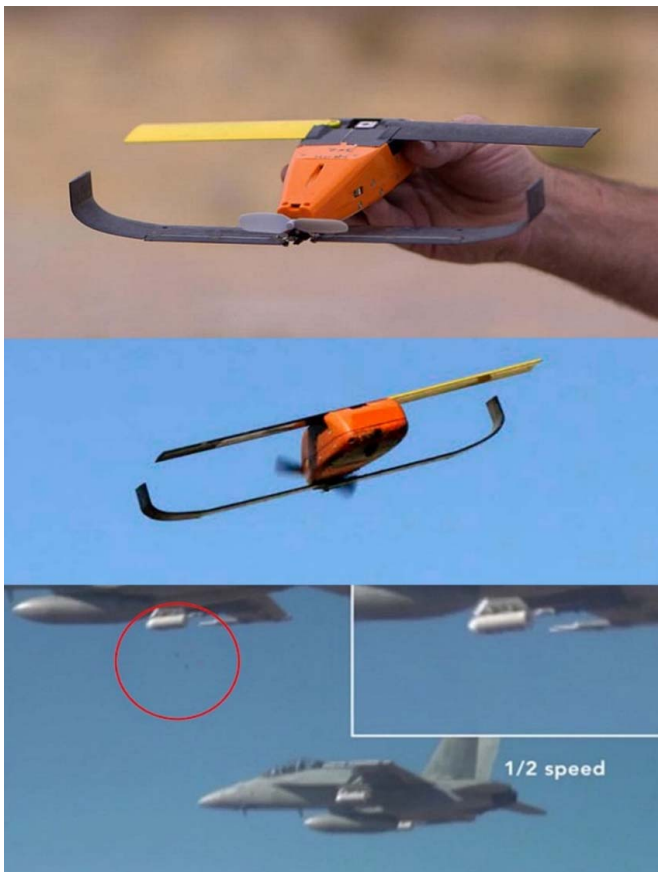

Figura 1. Dron Perdix. Fuente: http://www.newscast-pratyaksha.com/english/us-department-defense-successfully-tests-micro-drones-based-swarm-technology/

de la misión.

[35] Del inglés enjambre.

[36] Para más información: https://www.darpa.mil/program/gremlins

[37] Para más información: https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/

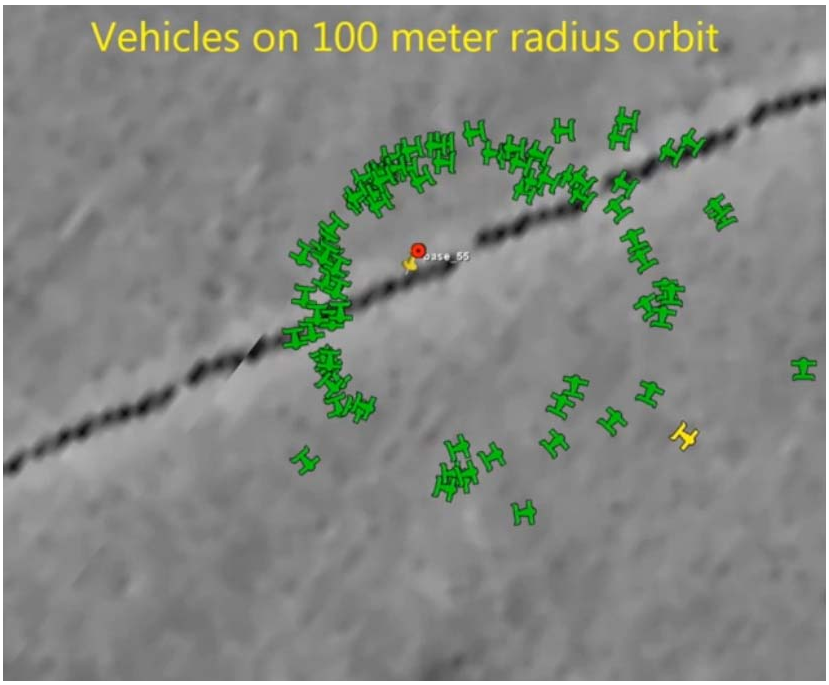

Figura 2. Drones Perdix realizando una misión colaborativa sobre un objetivo
Fuente: https://www.dvidshub.net/video/504622/perdix-swarm-demo-oct-2016

Efectividad

La efectividad es el equilibrio entre eficacia y eficiencia, se es efectivo si se es eficaz y eficiente. La eficacia es lograr un resultado o efecto y está orientado al que, en el caso de los sistemas de defensa aérea a neutralizar una amenaza. En cambio, eficiencia es la capacidad de lograr el efecto en cuestión con el mínimo de recursos posibles viable, o sea, el cómo[38].

La adquisición de un sistema de armas por parte de un Estado es un proceso lento y costoso. Los avances tecnológicos actuales son tales que en muchas ocasiones van por delante del ciclo de adquisición de un determinado sistemas de armas. Gran cantidad de sistemas de armas cinéticos para la defensa aérea de los países occidentales tienen carencias a la hora de acometer una amenaza tipo LSS UAS, ya que su concepción estaba basada en amenazas aéreas convencionales, por lo que su eficacia no es del todo óptima[39]. Desde hace años la industria armamentística está desarrollando nuevos sistemas de armas cinéticos optimizados no solo para amenaza convencional, sino

[38] https://es.wikipedia.org/wiki/Efectividad.
[39] HANS-WILHELM, Warnke, «Reconnaissance of LSS-UAS with Focus on EO-Sensors», STO-MP-SET-241, NATO, Germany.

también para amenaza tipo dron, como pueden ser el sistema *Patriot* y su misil PAC-3 MSE, el misil Stunner[40] o el sistema MANTIS[41] entre otros. La eficacia de un sistema de armas frente a una amenaza determinada se puede medir por la *Probability of kill* o Pk. La 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 (P_{hit}) o la probabilidad de detección de la amenaza (P_d) entre otros. Para los sistemas de armas cinéticos anteriormente vistos, un objetivo LSS UAS supone un verdadero reto por sus especiales características, por lo que la 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. Como datos reseñables los fabricantes de sistemas de armas ofrecen unos datos de Pk estimativos frente a ciertos blancos, como pueden ser el sistema *Skyshield* con cañones de 35 milímetros y munición AHEAD que asegura una Pk de 0,3 a 1.000 metros, 0,7 a 500 metros o 0,98 a 200 metros frente a LSS UAS[42].

Aun considerando una eficacia aceptable, para que sea efectiva necesitamos que la eficiencia sea a su vez elevada. Como hemos visto anteriormente, en términos económicos y de cantidad, la eficiencia es desfavorable en multitud de supuestos, por lo que deben buscarse alternativas. Como se verá con posterioridad, los sistemas de armas no cinéticos son el complemento que puede cubrir esa brecha.

Proceso de detección e identificación

Hasta ahora el documento se ha centrado en la parte vector del sistema de armas para neutralizar las amenazas aéreas, que es el objetivo principal del documento. Es obvio que para neutralizar una amenaza aérea primero debe ser detectada e identificada. Los LSS UAS representan un verdadero hándicap en los procesos de detección e identificación, ya que poseen capacidades furtivas, como pueden ser bajo RCS, baja firma térmica y acústica y patrones de vuelo que en muchos casos dificultan su detección[43]. Este problema es común tanto a sistemas de armas cinéticos como no cinéticos.

[40] Para más información: https://www.raytheon.com/capabilities/products/davidssling
[41] Para más información: https://www.army-technology.com/projects/mantis/
[42] Para más información: http://aviationweek.com/awin/basing-c-ram-system-close-home
[43] Para más información: http://www.ieee.es/Galerias/fichero/docs_marco/2018/DIEEEM03-

Se están desarrollando nuevos sistemas multisensor para detectar estas amenazas a la vez que nuevos sistemas y procesos de identificación[44]. La diferencia fundamental con los mismos procesos frente a amenazas convencionales es que frente a LSS UAS la ventana temporal para detectar, identificar y neutralizar es, en multitud de casos, extremadamente breve. Es por ello que muchos de los nuevos desarrollos abogan por sistemas de armas autónomos o semiautónomos[45], sistemas por otro lado más óptimos para armamento no cinético, por sus ventajas como el reducido daño colateral.

Defensa en profundidad

Como se vio con anterioridad, una de las premisas fundamentales de los SDA es la defensa en profundidad. Este concepto supone establecer una serie de barreras por medio de sistemas de armas, de tal manera que un supuesto enemigo deba sobrepasar cada una de esas barreras para cometer su acción hostil. La defensa en profundidad da al poder decisorio tiempo de reacción para poder ejercer el control de sus defensas y asignar sistemas de armas de manera jerarquizada en función de la situación táctica. En la imagen 3 está representada esta concepción, con la presencia de cazas y varios anillos con los diferentes alcances de supuestos sistemas antiaéreos.

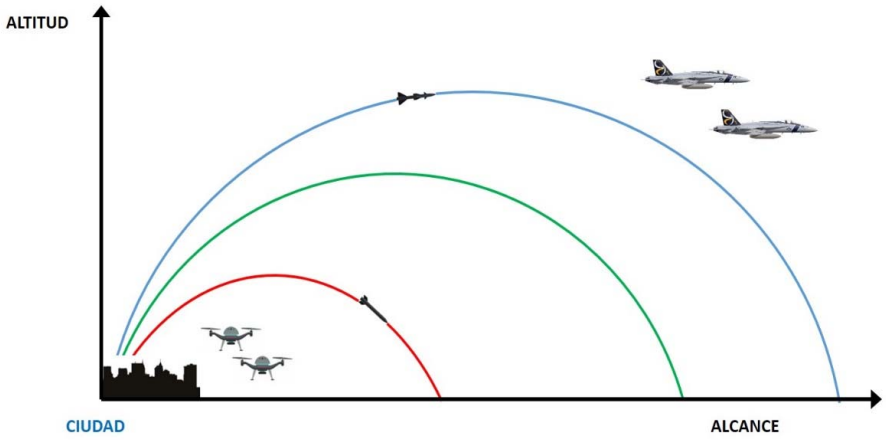

Figura 3. Representación defensa en profundidad. Elaborada por el autor

2018_DronesComerciales-VectoresTerroristas_JAMarinDelgado.pdf

[44] Para más información: Artículo, *«Drones, la nueva amenaza del espacio aéreo»*. http://www.ejercitodelaire.mde.es/EA/ejercitodelaire/es/.galleries/anexos/revista/RAA-Julio-Agosto.pdf

[45] El sistema Oerlikon Skyshield es un ejemplo de sistema autónomo. Para más información: https://www.rheinmetall-defence.com/en/rheinmetall_defence/systems_and_products/air_defence_systems/stationary_air_defence/index.php

Como se ha visto en el apartado anterior, los procesos de detección e identificación frente a LSS UAS son complejos y extremadamente breves en muchos casos. Otra de las características de los LSS UAS es su pequeño tamaño, por lo que pueden ser transportados fácilmente, es por ello que se puede prever su empleo incluso tras las líneas enemigas, algo que unido a lo anterior anula en gran medida la capacidad de defensa en profundidad y por ende el tiempo de reacción.

Por ejemplo, el dron chino CH-901[46] tiene un peso de 9,1 kilos, siendo 2,7 kilos de carga explosiva y es lanzado desde un tubo similar a un MANPADS[47]. Tiene un alcance de 15 kilómetros y alcanza una velocidad de entre 70 y 120 km/h. Empleado tras las líneas enemigas a 3 kilómetros de un objetivo como una base aérea, el citado dron «kamikaze» alcanzaría el objetivo en tan solo 90 segundos.

Al igual que en el caso anterior, la pérdida de la defensa en profundidad en casos como la amenaza LSS UAS debe ser cubierta por otros sistemas de armas.

Guerra Electrónica (EW)[48] y operaciones en el ciberespacio para la defensa aérea contra drones

Una de las diferencias de los sistemas aéreos no tripulados frente a los tripulados es su mayor dependencia del espectro electromagnético para su operación. Las aeronaves no tripuladas se enfrentan con mayor frecuencia a mayores riesgos que sus contrapartes tripuladas debido a vulnerabilidades en tres áreas principales: el enlace de datos para controlar la aeronave, el enlace de datos que proporciona información de los diferentes sensores de misión a la estación terrestre y la información proporcionada por el sistema global de navegación por satélite (GNSS)[49] al sistema de navegación que permite a la aeronave proporcionar datos posicionales precisos al operador[50]. A su vez y no menos importante es la total dependencia de computadores y software de control de estos artefactos.

[46] Para más información: http://smalldronesreview.com/2016/05/07/china-ch-901uav-drone-full-specifications/
[47] Del inglés *man portable air defense system*.
[48] Del inglés *electronic warfare*.
[49] Del inglés *global navigation satellite system.*
[50] HAY, Thomas E., «DETERMINING ELECTRONIC AND CYBER ATTACK RISK LEVEL FOR UNMANNED AIRCRAFT IN A CONTESTED ENVIRONMENT», AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, August 2016, Alabama, disponible en http://www.dtic.mil/dtic/tr/fulltext/u2/1040702.pdf.

Identificando estas dependencias se pueden emplear sistemas de armas para negar el uso de parte del espectro electromagnético o corromper su *software* o hardware de tal manera que se pueda neutralizar la amenaza con o sin destrucción física de la misma.

Los sistemas de armas no cinéticos en función del campo en el que operen van a estar encuadrados dentro de la denominada guerra electrónica o en el de las operaciones en el ciberespacio.

El término guerra electrónica se refiere a cualquier acción militar que involucre el uso de energía electromagnética y energía dirigida (DE)[51] para controlar el espectro electromagnético o para atacar al enemigo. La guerra electrónica está formada por tres divisiones: Ataque electrónico (EA)[52], protección electrónica (EP)[53] y apoyo (ES)[54]. Dentro de estas tres divisiones la que nos interesa en este estudio es el Ataque Electrónico. El ataque electrónico es el campo de la guerra electrónica que involucra el uso de energía electromagnética, energía dirigida o armamento antirradiación para atacar personal, instalaciones o equipos, con la intención de degradar, neutralizar o destruir la capacidad de combate del enemigo. Ejemplos de sistemas de armas en este campo son las armas de energía dirigida (DEW)[55] o sistemas de interferencia (*jamming*)[56].

Las operaciones en el ciberespacio son aquellas que emplean las capacidades de ciberespacio, es decir, el dominio global dentro del entorno de información que consiste en infraestructuras de redes interdependientes de tecnología de la información y datos residentes, incluyendo internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados, con el principal propósito de lograr los objetivos en o a través del ciberespacio[57]. Ejemplos de sistemas de armas en este campo son sistemas de *spoofing* o de *hackeo*[58].

Las operaciones de guerra electrónica y del ciberespacio están íntimamente relacionadas. Dado que el ciberespacio requiere enlaces por cable e inalámbricos para transportar información, las operaciones de ciberespacio tanto ofensivas como

[51] Del inglés *directed energy.*
[52] Del inglés *electronic attack.*
[53] Del inglés *electronic protection.*
[54] Del inglés *electronic support.*
[55] Del inglés *directed energy weapons.*
[56] Joint Publication 3-13.1
[57] Joint Publication 1-02
[58] Ambas técnicas se verán con posterioridad.

defensivas pueden requerir el uso del espectro electromagnético para producir efectos en el ciberespacio. Debido a la naturaleza complementaria y los posibles efectos sinérgicos de ambas, deben coordinarse para garantizar que se apliquen para maximizar la efectividad[59].

Sistemas de armas no cinéticos

Armas de energía dirigida (DEW)

El documento JP 1-02 define como arma de energía dirigida, un arma o sistema que usa energía dirigida para incapacitar, dañar o destruir equipamiento enemigo, instalaciones y/o personal. Existen diversos tipos de armas de energía dirigida, dos de los cuales tienen actualmente más aplicaciones en la defensa aérea no cinética: los láseres y los sistemas de armas de microondas de alta potencia (HPM)[60].

Sistema de armas láser

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. Estas características únicas del rayo láser lo hacen muy importante para aplicaciones militares[61].

La efectividad de las armas láser depende básicamente de la relación entre la dureza del objetivo, las distorsiones atmosféricas, la longitud de onda, la calidad del haz y la duración del láser. La capacidad de daño de un arma láser aumenta cuando la potencia de salida del arma y el tiempo de permanencia aumentan. Por otro lado, disminuye cuando las longitudes de onda del rayo láser y el rango aumentan[62].

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,

[59] Joint Publication 3-13.1.
[60] Del inglés *high power microwave*.
[61] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y
[62] Ibíd.

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[63].

Figura 5. Efectos producidos por un arma láser sobre un dron
Fuente: https://medium.com/war-is-boring/u-s-army-laser-chief-we-absolutely-blew-lots-of-stuff-up-a5c3a2f6a23c

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. La destrucción mecánica puede requerir menos energía para dañar o degradar el rendimiento de un objetivo que la destrucción térmica, pero requiere intensidades más altas y anchuras de pulso más cortas[64].

Existen tres tipos principales de láser: químicos (en desuso por su peso y necesidades logísticas), de estado sólido (SSL)[65] y láser de electrón libre (FEL)[66].

Los láseres se clasifican según su potencia de emisión máxima en kilovatios (kW). La potencia requerida para neutralizar objetivos LSS UAS, dependerá de diversos factores como distancia al objetivo, tiempo de exposición, condiciones meteorológicas o características del dron.

[63] Ibíd.
[64] Ibíd.
[65] Del inglés *solid-state laser.*
[66] Del inglés *free-electron laser.*

POTENCIA LÁSER (Kw)	GRUPO
2-5	1
10-15	2
+30	**3**

Tabla 5. Potencia requerida para neutralizar LSS UAS. Elaborada por el autor. Fuente: https://tradocnews.org/with-no-bullets-mobile-high-energy-laser-shoots-drones-from-sky/.

Capacidades

a) Los sistemas de armas láser suponen una reducción drástica de los costes tanto de adquisición, como de operación y empleo. En cuanto a los costes de adquisición, estos sistemas son mucho más económicos que la mayoría de sistemas de armas cinéticos, ya que parte de la tecnología láser procede del mercado civil. Por otro lado, los costes de operación son inferiores a los sistemas cinéticos ya que las necesidades logísticas son muy inferiores. Y en cuanto al empleo, es una de las mayores ventajas, ya que el coste de cada disparo se reduce al coste de la energía eléctrica requerida por el sistema. Durante el ejercicio MFIX 2016, el sistema de armas MEHEL (*Mobile Expeditionary High Energy Laser*) derribó un LSS UAS a un costo de 30 dólares, que corresponde con el precio aproximado del diésel consumido para generar cada disparo[67].

b) Es un concepto de sistemas de armas con mantenimiento y piezas de repuesto reducido. La carencia de municiones alivia la carga de trabajo logística a la vez que anula el riesgo de la operación de esta a los operadores. Estas características los hacen sistemas con grandes capacidades expedicionarias[68].

c) 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. Otra de sus características es que puede reorientarse rápidamente pasando de un objetivo a otro variando la orientación de sus espejos. A su vez el haz láser es extremadamente estrecho y preciso, por lo que el riesgo de daño colateral o daño a fuerzas propias se reduce enormemente, algo vital en entornos congestionados como ciudades[69].

[67] «Warfighter Experimentation with High Energy Lasers (WEHEL) Fact Sheet», US Army Space and Missile Defense Command, disponible en https://www.smdc.army.mil/FactSheets/WEHEL.pdf.
[68] PUDO, Dominic y GALUGA, Jake, «High energy laser weapon systems: evolution, analysis and perspectives», Defence Research and Development Canada (DRDC), Canadian Military Journal, july 2017, Canada.
[69] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en

d) 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[70]. En sistemas láser instalados en grandes plataformas como buques, en los que la disponibilidad de corriente eléctrica y refrigeración no es un problema, el número de disparos puede ser casi ilimitado. En plataformas más reducidas como vehículos terrestres el número de disparos se reducirá[71]. En este sentido, se están desarrollando nuevos generadores y baterías más eficientes para asegurar un suministro óptimo en cualquier entorno[72].

e) Los sistemas de armas láser son extremadamente flexibles y modulares. Una particularidad es que pueden unirse distintos módulos para crear láseres de mayor potencia o por otro lado ser adaptados a diferentes tipos de plataformas en función de sus características. A su vez pueden utilizarse para batir multitud de objetivos además de los aéreos, como vehículos terrestres, barcos o RAM[73].

f) 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. Los sistemas de armas cinéticos en una escalada de tensión emplearían disparos de advertencia como primera medida disuasoria, algo que el láser puede aplicar variando su potencia. Su potencia ajustable unida a su direccionalidad permiten seleccionar dentro de un objetivo el sistema o localización donde atacar. Por ejemplo poder inhabilitar un sensor concreto como la cámara IR[74] de un dron sin tener que derribarlo[75].

https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y

[70] Por ejemplo un láser tipo SSL con una eficiencia energética aproximada del 25 %. Por cada kilovatio de energía que proyecta, hay 3 kilovatios de calor que deben ser disipados. Fuente: https://calhoun.nps.edu/bitstream/handle/10945/42734/14Jun_Sylvester_Jeremy.pdf;sequence=1

[71] DUNN, Richard J., «Operational Implications of Laser Weapons», Analysis Center Paper, September 2005, disponible en https://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/Operational_Implications_of_La.pdf

[72] Por ejemplo la empresa Leonardo DRS dispone de soluciones tecnológicas para solucionar la gran demanda de energía de las armas láser. https://defensesystems.com/articles/2017/01/23/fabeylaser.aspx

[73] Del inglés *rockets, artillery and mortars*. Cohetes, artillería y morteros.

[74] Del inglés *infra-red*.

[75] PUDO, Dominic y GALUGA, Jake, «High energy laser weapon systems: evolution, analysis and perspectives», Defence Research and Development Canada (DRDC), Canadian Military Journal, july 2017, Canada.

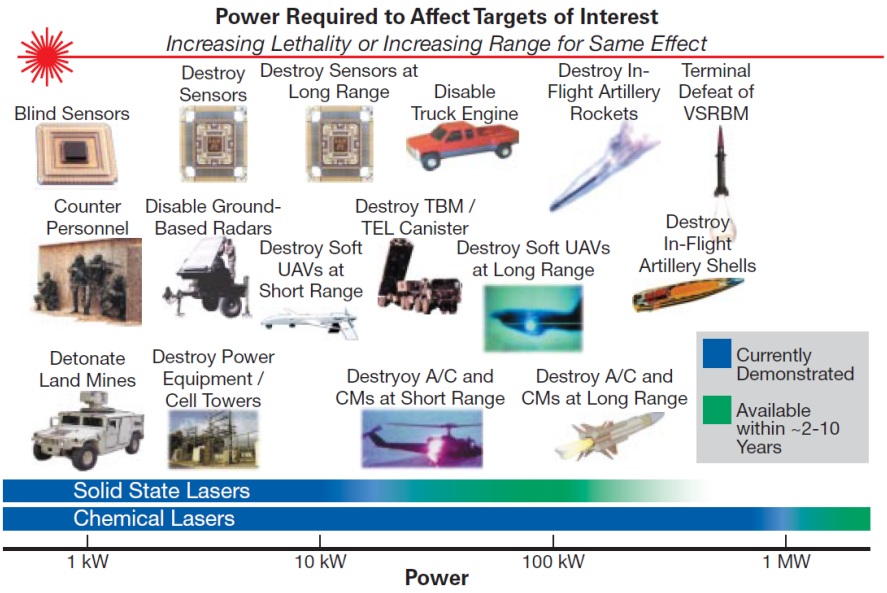

Figura 6. Potencia requerida para dañar a objetivos de interés. Fuente: https://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/Operational_Implications_of_La.pdf

Limitaciones

a) 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[76]. Esta limitación hace que sus alcances sean relativamente discretos frente a otros sistemas de armas cinéticos, por lo que sus aplicaciones en la actualidad se limitan a encuadrarse en defensas de corto y muy corto alcance. La industria está realizando grandes avances con sistemas de ópticas adaptativas (AO)[77], de tal manera que el sistema identifica las condiciones atmosféricas y compensa los parámetros del haz láser para un alcance óptimo[78]. Por ejemplo, el prototipo láser de alta energía (HEL) de la compañía Rheinmetall ha conseguido alcances de hasta 3.000 metros[79], alcance muy discreto

[76] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y

[77] Del Inglés *adaptive optics.*

[78] Para más información: http://www.northropgrumman.com/Capabilities/LaserTechnology/Pages/BeamControl.aspx

[79] Para más información: https://www.rheinmetall.com/en/rheinmetall_ag/press/themen_im_fokus/zukunftswaffe_hel/index.php

comparado con el del misil 40N6 del sistema ruso S-400, con un alcance estimado de 400 kilómetros[80].

b) Existen materiales resistentes a la acción del láser, por lo que podría ser inefectivo frente amenazas revestidas de materiales que reflejen la energía láser. Científicos chinos están desarrollando revestimientos antiláser. En palabras del profesor Huang Chenguang de la Academia China de Ciencias, «…no importa cómo de potente o destructivo es (el láser), estará compuesto de luz que puede ser desviada por varios materiales»[81].

c) Un arma láser, a diferencia de gran multitud de sistemas de armas cinéticos[82], necesita mantener constantemente la línea de visión sobre el objetivo[83]. Frente a objetivos de trayectoria parabólica o en lugares con presencia de obstáculos como ciudades, su acción se puede ver degradada. Además de mantener la línea de visión es necesario iluminar al objetivo durante un tiempo que dependerá de la potencia del láser y de las características del objetivo. Este tiempo de iluminación puede ser insuficiente para amenazas detectadas a muy corta distancia[84].

d) A diferencia de otros sistemas de armas el láser 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.

e) La potencia alcanzada hasta ahora en los sistemas de armas láser es insuficiente para amenazas aéreas del grupo 3 y superior. El avance en este campo va a buen ritmo y se esperan alcanzar potencias superiores a 100 kW en un breve espacio de tiempo[85]. Esta falta de potencia es reseñable si se compara con el poder destructivo de

[80] Para más información: https://www.army-technology.com/projects/s-400-triumph-air-defence-missile-system/
[81] https://www.scmp.com/news/china/article/1444732/us-lasers-pla-preparing-raise-its-deflector-shields
[82] Gran número de misiles antiaéreos siguen trayectorias de navegación proporcionales, es decir, en su desplazamiento al objetivo mantiene una trayectoria sobre el punto de impacto futuro. Esto permite hacer uso del armamento aunque no se tenga línea de visión con el objetivo. Para más información: https://nptel.ac.in/courses/101108056/module5/lecture9.pdf
[83] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y
[84] DUNN, Richard J., «Operational Implications of Laser Weapons», Analysis Center Paper, September 2005, disponible en https://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/Operational_Implications_of_La.pdf
[85] https://breakingdefense.com/2018/08/its-raytheon-vs-dynetics-lockheed-for-armys-100-kw-laser/

explosivos como el TNT. La energía liberada por un láser de 100 kW es de 100 kJ por segundo, un kilo de TNT libera 47 veces más energía[86].

Ejemplos de sistemas de armas láser

Los sistemas de armas láser se están integrando en plataformas navales, terrestres, aéreas e incluso espaciales. Ejemplos de estos sistemas son:

a) *Boeing YAL-1 / ABL (Airbone Laser):* El ABL fue un proyecto de láser aéreo embarcado desarrollado para contrarrestar la amenaza de misiles balísticos. El láser de tipo químico COIL[87], fue integrado en una aeronave Boeing 747-400F. Su potencia máxima era del orden de los megavatios[88]. El proyecto cancelado en 2012 sirvió como banco de pruebas para posteriores desarrollos.

b) *AN/SEQ-3 Laser Weapon System (XN-1 LaWS):* Este láser de tipo SSL fue instalado en el buque norteamericano USS PONCE en el año 2014. El sistema fue probado exitosamente frente a objetivos aéreos como drones ScanEagle, granadas propulsadas o botes ligeros. La potencia nominal máxima era de 30 kW y el costo estimado por disparo de 59 céntimos de dólar. El buque ha sido dado de baja el presente año y se prevé instalar una evolución del citado láser mucho más potentes en navíos más modernos con sistemas de generación de potencia[89] de mayor capacidad[90].

[86] PUDO, Dominik y GALUGA, Jake, «High Energy Laser Weapon Systems: Evolution, Analysis and Perspectives», Canadian Military Journal, summer 2017, disponible en http://www.journal.forces.gc.ca/Vol17/no3/PDF/CMJ173Ep53.pdf

[87] Del inglés *chemical oxygen iodine laser*.

[88] Para más información: http://www.northropgrumman.com

[89] La relación de potencia emitida frente a potencia requerida en el citado láser es de 1:3. Es por ello por lo que se necesitan generadores de energía de gran capacidad.

[90] «Laser- The weapon of the future», Global Military Communications Magazine, october 2017, disponible en http://www.satelliteevolutiongroup.com/articles/Laser-weapons-2017.pdf

Figura 7: Boeing YAL-1. Fuente: https://en.wikipedia.org/wiki/Boeing_YAL-1

En marzo del presente año la empresa Lockheed Martin ha sido galardonado con un contrato para la fabricación de dos sistemas de armas láseres. El contrato contempla la instalación para el año 2020 de un sistema láser en un destructor de la clase Arleigh Burke y otro sistema en el polígono de pruebas de *White Sands*[91].

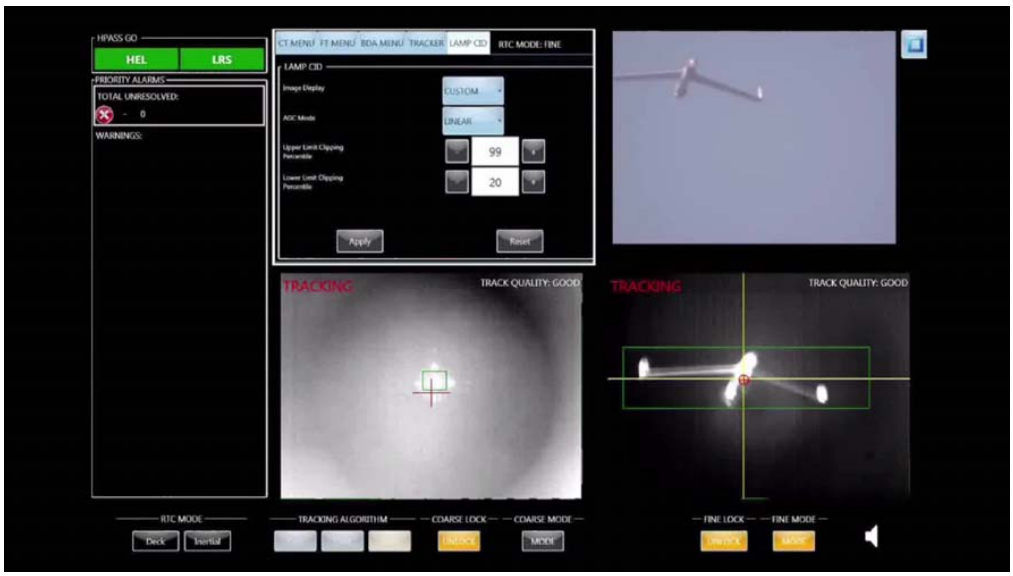

Figura 8: Imagen del puesto de operador del Laser XN-1 LaWS en el USS PONCE destruyendo un dron ScanEagle. Fuente: https://www.hqmc.marines.mil/News/MarinesTV/videoid/381080/dvpTag/critical/

c) *MEHEL*: El MEHEL es un sistema de armas láser montado sobre un vehículo 8x8 Stryker concebido para amenaza UAS y RAM. Equipado inicialmente con un láser SSL de 2 kW fue capaz de derribar más de 15 LSS UAS durante el ejercicio MFIX

91 https://news.lockheedmartin.com/2018-03-01-Lockheed-Martin-Receives-150-Million-Contract-to-Deliver-Integrated-High-Energy-Laser-Weapon-Systems-to-U-S-Navy

2016. La evolución del sistema conocido como MEHEL 2.0 porta un láser de 5 kW y, al igual que su predecesor, fue capaz de derribar numerosos LSS UAS en el ejercicio *UAS Hard-Kill Challenge* de la JIDO[92] a principios de 2017[93]. Se estima que la próxima evolución de este sistema alcance una potencia de 10 kW[94].

Figura 9: Sistema de armas MEHEL. Fuente: http://www.dmitryshulgin.com/wp-content/uploads/2017/04/Stryker.jpg

d) *Rheinmetall HEL*: El láser de alta energía de la compañía europea Rheinmetall, ha sido desarrollado para ser instalado en diferentes plataformas con una configuración de potencia máxima variable en función de la misma. Se ha integrado en el sistema de defensa Skyshield, con una potencia de 30 kW, obteniendo alcances frente a drones y munición de mortero de hasta 3.000 metros. En un escenario simulado contra LSS UAS fue capaz de neutralizar el sistema electroóptico de un dron de reconocimiento y posteriormente derribar 3 drones tipo jet[95].

[92] Del inglés *Joint Improvised-Threat Defeat Organization*.

[93] https://www.army.mil/article/184353/army_demonstrates_integration_of_laser_weapon_on_combat_vehicle

[94] https://breakingdefense.com/2017/07/army-boosting-laser-weapons-power-tenfold/

[95] https://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/themen_im_fokus/rheinmetall_hel_live_fire/#

e) *Otros programas*

1. El AFRL adjudicó a la empresa Lockheed Martin un contrato por valor de 26,3 millones de dólares para desarrollar y producir un láser de alta potencia para ser instalado en aviones de caza en el 2021. El programa se denomina *Self-Protect High-Energy Laser Demonstrator* (SHiELD)[96].
2. El USSOCOM[97] y la empresa Raytheon probaron a mediados de 2017 un sistema láser acoplado a un helicóptero AH-64 Apache. El sistema fue efectivo contra objetivos estacionarios hasta una distancia de 1.400 metros y marca el camino de próximas evoluciones[98].

Figura 10. Detalle del sistema láser de Raytheon en un AH-64. Fuente: https://www.avweb.com/avwebflash/news/Raytheon-Testing-Helicopter-Laser-Weapon-229219-1.html

3. La Agencia Europea de Defensa identificando las posibilidades de las DEW y analizando las carencias del conjunto de la Unión Europea en esta materia (la máxima potencia láser conseguida por un país del Viejo Continente ha sido 50 kW) lanzó en marzo de este año el PADR-EF-02-2018[99] para el desarrollo de un láser de 100 kW, con un presupuesto de 5,4 millones de euros[100].
4. Además de los sistemas o proyectos enumerados con anterioridad, existen numerosos desarrollos como el *Iron Beam*[101] israelí o el *Silent Hunter*[102] chino,

[96] https://news.lockheedmartin.com/2017-11-06-Lockheed-Martin-Receives-Contract-to-Develop-Compact-Airborne-High-Energy-Laser-Capabilities
[97] Del inglés *United States special operations command.*
[98] https://www.raytheon.com/news/feature/high_energy_laser
[99] PADR del inglés *preparatory action on defence research*.
[100] http://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/wp-call/pa-call-document-padr-fss-18-call-text_en.pdf
[101] https://en.wikipedia.org/wiki/Iron_Beam
[102] https://www.businessinsider.com/china-laser-weapons-2018-5?IR=T#2-the-silent-hunter-2

que demuestran la importancia de este tipo de sistemas de armas para la defensa en los próximos años.

Sistemas de armas de microondas de alta potencia (HPM)

Las microondas de alta potencia, en adelante HPM, 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. Aunque el término microondas técnicamente solo se aplica a las ondas de radio de frecuencia más alta, es decir, aquellas que operan en el rango de gigahercios, se ha vuelto común hacer referencia a todas las armas de energía dirigida que funcionan en frecuencias de radio como HPM[103].

Las armas HPM generalmente se subcategorizan como sistemas de banda estrecha (NB)[104] o banda ultra ancha (UWB)[105].

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[106].

La energía de HPM puede afectar a cualquier cosa que responda a tensiones y corrientes inducidas electromagnéticamente. Dos mecanismos se producen en objetos bajo un haz de HPM: calentamiento molecular y estimulación eléctrica. Una vez que la energía de microondas alcanza un objetivo, se llevará a cabo una secuencia de procesos de

[103] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y

[103] Para más información: https://www.defensenews.com/digital-show-dailies/smd/2018/08/10/sweden-locked-in-to-buy-patriot-missile-defense-system/

[104] Del inglés *narrow band*.

[105] Del inglés *ultra-wide band*.

[106] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y

[106] Para más información: https://www.defensenews.com/digital-show-dailies/smd/2018/08/10/sweden-locked-in-to-buy-patriot-missile-defense-system/

penetración y propagación desde la superficie exterior del objetivo hasta su interior. El calentamiento molecular es el resultado de armas HPM de banda estrecha en la superficie exterior del objetivo. Las moléculas del objetivo se frotan debido a la potencia de la energía de microondas. La potencia requerida para obtener este efecto es bastante grande y es necesario un tiempo de permanencia significativo en el objetivo deseado[107].
El otro mecanismo eficiente tiene lugar cuando la energía de microondas finalmente llega a los componentes electrónicos del objetivo. Los sistemas de armas de microondas tienen la capacidad de producir efectos graduales en los componentes electrónicos del objetivo, dependiendo de la cantidad de energía que se acopla al mismo. El acoplamiento comienza con una respuesta exterior en sistemas protegidos como aviones, tanques y otros objetivos. Más tarde, la energía que se recibe puede transmitirse más profundamente en la electrónica a través de las rutas de circuitos que existen dentro del objetivo. El nivel de potencia y el tiempo de permanencia requeridos para la estimulación eléctrica son mucho menores que para el calentamiento molecular, lo que permite un mayor rango de acoplamiento[108].
Dependiendo del acoplamiento, los efectos de HPM pueden variar desde la degradación del sistema hasta la destrucción del mismo. Para la estimulación eléctrica o la penetración en el objetivo, las armas de microondas de alta potencia utilizan dos mecanismos de acoplamiento diferentes:

- El acoplamiento de «puerta delantera»[109] penetra en el objetivo a través de su propia antena, que está diseñada para recibir microondas, como antenas de comunicación, de radar o de altímetro.
- El acoplamiento de «puerta trasera»[110] es un mecanismo más complejo y se refiere a cualquier acoplamiento de radiación que no utiliza las antenas para penetrar en el objetivo, como pueden ser ventanas, ranuras, costuras, grietas o huecos insuficientemente apantallados[111].

[107] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y
[108] Ibíd.
[109] Del inglés f*ront-door coupling*.
[110] Del inglés *back-door coupling*.
[111] MERT, Bayram, «DIRECTED-ENERGY WEAPONS: INVISIBLE AND INVINCIBLE?», NAVAL POSTGRADUATE SCHOOL, September 2007, California, disponible en https://calhoun.nps.edu/bitstream/handle/10945/3311/07Sep_Deveci.pdf?sequence=1&isAllowed=y

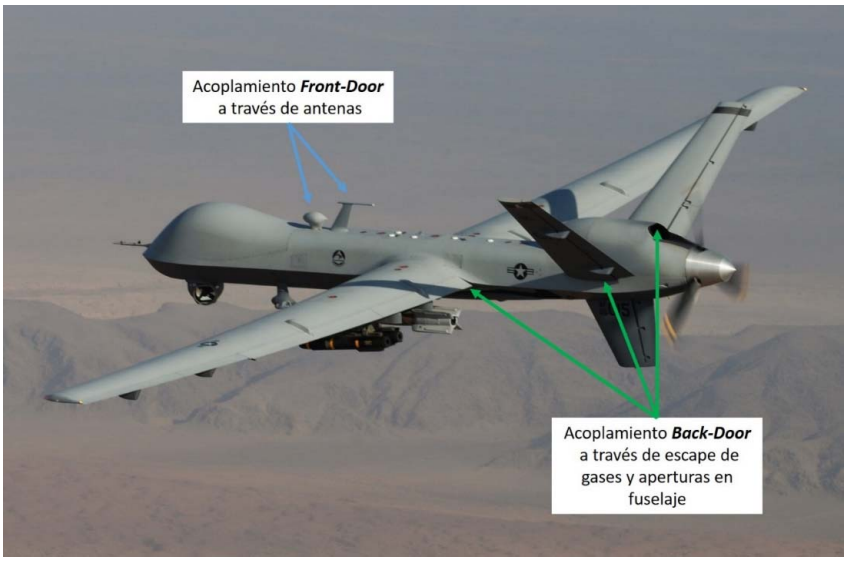

Figura 11: Acoplamiento de HPM sobre dron. Elaborada por el autor. Fuente: *U.S. Air Force*

En cuanto al daño producido por las armas HPM sobre los componentes electrónicos, el *Air Force Research Laboratory* (AFRL) establece 5 categorías o niveles[112]:

1. *Sin efecto (No effect)*: No se produce daño.
2. *Interferencia (Interference*): Produce un efecto mínimo cuando está iluminado.
3. *Alteración (Disturbance*): Afecta al sistema mientras se ilumina, pero se recupera.
4. *Perturbación (Upset*): Requiere intervención externa.
5. *Daño (Damage*): Requiere reemplazar el *software*, *hardware* o *firmware*.

Capacidades

a) Las armas HPM, al igual que las armas láser, son una opción económica en comparación con los sistemas de armas cinéticos. El coste de cada disparo se reduce al coste de la energía eléctrica requerida por el sistema y el número de disparos dependerá del suministro de energía eléctrica. Por otro lado, su carga logística es reducida y carecen de munición, por lo que anula el riesgo de su operación.

[112] BURDON, Coningsby J., «HARDENING UNMANNED AERIAL SYSTEMS AGAINST HIGH POWER MICROWAVE THREATS», AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, April 2017, disponible en http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwj4j_-S7_ncAhXSyqQKHeRFD34QFjAAegQIAhAC&url=http%3A%2F%2Fwww.dtic.mil%2Fget-tr-doc%2Fpdf%3FAD%3DAD1042082&usg=AOvVaw13kJHdXTRsS_d9uOO2DZ-c

b) Como arma electromagnética su acción es casi instantánea. A diferencia del láser no le afectan las condiciones atmosféricas para su operación. Se puede utilizar en entornos urbanos, e incluso sobre objetivos protegidos o bunquerizados[113].

c) 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 drones[114].

d) Permiten diferentes efectos sobre los objetivos dependiendo de la potencia de emisión, como se vio anteriormente. Incluso pueden producir daños en equipos apagados.

Limitaciones

a) 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[115].

b) 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. Este tipo de contramedidas son costosas, complejas y pueden aumentar la detectabilidad, como el RCS, por lo que su aplicación en LSS UAS se asemeja difícil[116].

c) 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[117].

d) Otras de las desventajas de las HPM es que emiten una firma electrónica fácilmente localizable, por lo que pueden delatar la posición al enemigo y ser objeto de ataque por parte de este[118].

---

[113] BURDON, Coningsby J., «HARDENING UNMANNED AERIAL SYSTEMS AGAINST HIGH POWER MICROWAVE THREATS», AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, April 2017.
[114] Ibíd.
[115] CAPOZZELLA, Robert J., «High power microwaves on the future battlefield: implications for U.S. defense», Air War College, February 2010.
[116] BURDON, Coningsby J., «HARDENING UNMANNED AERIAL SYSTEMS AGAINST HIGH POWER MICROWAVE THREATS», AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, April 2017.
[117] CAPOZZELLA, Robert J., «High power microwaves on the future battlefield: implications for U.S. defense», Air War College, February 2010.
[118] BAILEY, Branden G., «Offseting tomorrow´s adversary in a contested enviroment: defending expeditionary advance bases in 2025 and beyond», Air War College, April 2017.

Ejemplos de sistemas de armas HPM

Los sistemas de armas HPM al igual que los láseres se están integrando en todo tipo de plataformas. Ejemplos de estos sistemas son:

a) *RANETS-E:* El RANETS-E es un sistema de armas de defensa aérea de HPM ruso, revelado por Rosoboronexport en 2001. Esta arma usa HPM pulsado de 500 megavatios en la banda X. Se estima un alcance letal de 20 millas para objetivos no protegidos. En caso de objetivos protegidos su rango de acción se reduciría por debajo de 10 millas[119].

b) *PHASER:* El Phaser es un arma HPM diseñada por Raytheon de tipo modular instalada en un contenedor de 20 pies con sistema propio de generación de energía. Este sistema permite al operador dañar o destruir drones de categoría 1 y 2. Entre septiembre y octubre de 2013 el prototipo de este sistema derribó 2 drones de manera casi instantánea en un polígono de tiro de Oklahoma. En el ejercicio MFIX 2018 Raytheon confirmó que este sistema derribó enjambres de dos y tres drones de manera simultánea[120]. Raytheon afirma que ha reducido el tamaño del sistema a la mitad y ofrece esta arma lista para su uso operacional[121].

Figura 12. Sistema Phaser. Fuente: https://nworeport.me/2018/03/25/high-energy-lasers-and-microwave-anti-drone-weapons-will-be-a-multi-billion-market-by-2023/

[119] http://www.ausairpower.net/APA-Rus-PLA-PD-SAM.html#mozTocId210606
[120] https://www.popularmechanics.com/military/research/a19599393/watch-microwave-and-laser-weapons-knock-drones-out-of-the-sky/
[121] https://www.uasvision.com/2016/11/18/raytheons-high-power-microwave-weapon-downs-drones/

c) *HPEMcounterUAS*: Este sistema de HPM forma parte del sistema C-UAS GUARDION. Por medio de HPM ataca los semiconductores de los circuitos electrónicos inhabilitándolos. Puede utilizarse a diferentes distancias y contra grupos de drones. Fue empleado en la cumbre del G7 en Alemania en el año 2015 de manera exitosa[122].

d) *Counter-electronics High Powered Advanced Missile Project (CHAMP):* El AFRL junto con la empresa Boeing han desarrollado este sistema de HPM para ser montado en misiles de crucero. Este concepto permite el uso de su sistema de HPM a larga distancia, durante periodos prolongados sobre grandes áreas. Puede ser usado frente a enjambres de drones o frente a cualquier sistema electrónico del enemigo con un daño colateral mínimo. Este sistema fue probado satisfactoriamente en octubre de 2012, usando como vector un misil AGM-86. El AFRL ha designado como vector final para el CHAMP el AGM-158B JASSM-ER[123] de *Lockheed Martin*, misil de crucero con más de 600 millas de alcance, que puede ser portado tanto por cazas como el F/A-18 o F-35 como por bombarderos[124].

Figura 13. Sistema HPEMcounterUAS. Fuente: https://armadainternational.com/2018/07/debut-of-diehls-counter-uas-effector-at-eurosatory/

[122] https://www.drohnenabwehr.de/en/integrated-system/effectors/hpem/
[123] Del inglés joint air-to-surface standoff missile.
[124] PA, Patil, «COUNTER-ELECTRONICS HIGH-POWERED MICROWAVE ADVANCED MISSILE PROJECT», Centre for Air Power Studies (CAPS), May 2015, disponible en http://capsindia.org/files/documents/CAPS_Infocus_PP_12.pdf

Figura 14. Detalle de un misil JASSM. Fuente: http://www.ejercitos.org/jassm_er_1_pl/

e) *Otros programas:*

1. El USACC[125] ha anunciado la intención de solicitar y negociar el desarrollo de drones C-UAS[126] con sistema de armas de HPM a la empresa Lockheed Martin[127].
2. Países como China están desarrollando sistemas de armas basados en tecnología HPM, como el Programa 863. Este país podría haber obtenido conocimiento tecnológico en este campo de los desarrollos rusos RANETS-E y ROSA-E[128].

Interferencia electromagnética (Electromagnetic Jamming)

La interferencia es uno de los grandes problemas presentes en los sistemas de telecomunicaciones. En general, la interferencia puede ser vista como una señal no deseada dentro del rango de operación de un determinado sistema de comunicación. Como bien sabemos, 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

[125] Del inglés *US Army Contracting Command*.
[126] Del inglés *counter ummaned aerial system.*
[127] https://www.unmannedairspace.info/counter-uas-systems-and-policies/lockheed-martin-provide-us-army-airborne-c-uas-payloads/
[128] FISHER, Richard D., «China's Progress with Directed Energy Weapons», February 2017, Washington, D.C., disponible en https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf

interferencia, se tendrá una reducción de esa relación y, consecuentemente, una degradación en la calidad de la comunicación. Este trabajo se centrará en la interferencia del tipo radiofrecuencia (RF), lógicamente causada por señales de RF en la misma frecuencia de operación del sistema interferido o en frecuencias cercanas. Las interferencias intencionales son aquellas generadas de forma intencional, a fin de inviabilizar el establecimiento de enlaces de comunicación en determinadas frecuencias. Como vimos anteriormente son un tipo de AE y dentro de las mismas veremos el *Electromagnetic Jamming* (en adelante *Jamming*)[129].

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 enemigo[130].

Existen diferentes tipos de *jamming*, como el *tone*, *pulse*, *sweep* o el *protocol-aware* entre otros[131]. Su efectividad dependerá de la técnica usada y de las características del objetivo.

Los drones por norma general si son controlados a distancia están transmitiendo señales de RF, bien sean de control, de vídeo 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. Es por ello que el *jamming* contra estos artefactos se ejercerá sobre la señal GNSS en caso de vuelo autónomo o sobre las señales del link de datos en caso de vuelo por control remoto.

Gran número de drones y la gran mayoría de drones de uso comercial tienen un dispositivo de seguridad que, en caso de sufrir interferencias en su link de datos o en la recepción de la señal del GNSS, volverían al punto de origen programado por el operador[132] o describirían una trayectoria específica intentando recuperar señal o bien aterrizarían sobre el lugar donde sufrieron la interferencia.

[129] VALIM, Rodrigo L. y DOS ANJOS, André, «Estudo e Simulação de Diferentes Tipos de Interferidores em Sistemas de Comunicação Digital», SEMINÁRIO DE REDES E SISTEMAS DE TELECOMUNICAÇÕES INSTITUTO NACIONAL DE TELECOMUNICAÇÕES, Julho 2017.
[130] *Joint Publication* 3-13.1.
[131] PALIN, Karel, «JAMMING OF SPREAD SPECTRUM COMMUNICATIONS USED IN UAV REMOTE CONTROL SYSTEMS», School of Information Technologies Thomas Johann Seebeck Department of Electronics, TALLINN UNIVERSITY OF TECHNOLOGY, 2017, Tallinn.
[132] Esta característica se conoce como *return to home* (R2H).

Jamming link de datos

Este tipo de sistemas de armas buscan interferir sobre la comunicación entre dron y operador. El enlace radioeléctrico entre dron y operador es principalmente de dos tipos: dentro de la línea de visión (LoS)[133] o más allá de la línea de visión (BLoS)[134]. A su vez si son operados de manera remota requieren al menos dos link de comunicaciones: un link de datos de vídeo (VDL)[135] y un link común de datos (CDL)[136,137]. Las bandas de frecuencia en las que operan son diversas y la explotación de las mismas está supeditada a nivel mundial a la Unión Internacional de Telecomunicaciones, sector radiocomunicaciones (UIT-R), la Comisión Europea a nivel europeo y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) a nivel nacional. Dependiendo del tipo de control LoS o BLoS[138], tipo de dron civil o militar o incluso las regiones de operación, las bandas de trabajo pueden ser diferentes. Son muy comunes las bandas de 2.4 GHz (ISM)[139] y 5.8 GHz para drones de uso comercial[140].

Capacidades

a) Como arma electromagnética su acción es casi instantánea. Por otro lado son sistemas muy económicos y efectivos frente a amenazas no protegidas.
b) Hay disponibles sistemas de *jamming* tanto direccionales para una amenaza localizada, como omnidireccionales para cubrir grandes áreas, como se verá más adelante.
c) Estos sistemas permiten una acción dirigida pudiendo atacar el enlace de datos de vídeo, telemetría, control, es decir, sobre su VDL o CDL.
d) Este tipo de sistemas de armas por norma general neutralizan la amenaza sin destruirla. En este sentido puede permitir capturar el dron enemigo (por ejemplo, si el

[133] Del inglés *line of sight*.
[134] Del inglés *beyond line of sight*.
[135] Del inglés *video data link*.
[136] Del inglés *common data link*.
[137] YOCHIM, Jaysen A., «THE VULNERABILITIES OF UNMANNED AIRCRAFT SYSTEM COMMON DATA LINKS TO ELECTRONIC ATTACK», Master of Military art and Science, 1998, Utah.
[138] Este tipo de operación puede requerir comunicaciones vía satélite.
[139] Del inglés *industrial, scientific and medical*. Son bandas reservadas en las áreas industrial, científica y médica. Son las utilizadas en comunicaciones Wifi o WPAN entre otras. Para más información: https://es.wikipedia.org/wiki/Banda_ISM
[140] «Jornada RPAS retos y oportunidades. Comunicaciones y espectro radioeléctrico. Visión de la Administración», Subdirección General de Planificación y Gestión del Espectro Radioeléctrico, septiembre 2015, disponible en http://www.aerpas.es/wp-content/uploads/2015/10/SETSI-Aeronaves-no-tripuladas-o-drones_V14_Vision-de-la-Admon.pdf

dron entra en modo pérdida de link y efectúa aterrizaje de emergencia) o incluso localizar al operador en el caso de LSS UAS (por ejemplo persiguiendo a un dron en situación de *Return to Home* R2H).

e) Son altamente flexibles pudiéndose instalar en localizaciones fijas o móviles. Existen sistemas de armas *jamming* que pueden ser portados por un operador con autonomía de varias horas y posibilidad de recarga, como se verá con posterioridad.

Limitaciones

a) Las bandas de RF en las que operan son utilizadas por sistemas de telefonía móvil, telecomunicaciones o redes Wifi entre otros, por lo que su acción puede afectar a sistemas propios o sistemas no deseados. Por ejemplo utilizando un *jamming* de barrera sobre cierta área.

b) En diversos países hay bandas de frecuencia que están protegidas, por lo que su interferencia solo puede ser autorizada por el Gobierno[141]. El uso de esas frecuencias protegidas para controlar LSS UAS con fines hostiles puede limitar la acción de estos sistemas de armas.

c) Actualmente existen multitud de desarrollos tecnológicos tanto civiles como militares para evitar las interferencias en su sistema de comunicación. Un ejemplo de esta tecnología es el Futaba Advanced Spread Spectrum Technology (FASST)[142], un sistema comercial de comunicaciones por salto de frecuencia, compatible con drones como el DJI Phamtom, capaz de soportar varios tipos de *jamming*[143].

d) Dado un caso de *jamming* sobre una amenaza LSS UAS 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.

---

[141] https://www.gps.gov/spectrum/jamming/
[142] Para más información: https://horejsi.cz/DataFilesEN/Futaba/Rx_R6008HS_EN.pdf
[143] PALIN, Karel, «JAMMING OF SPREAD SPECTRUM COMMUNICATIONS USED IN UAV REMOTE CONTROL SYSTEMS», School of Information Technologies Thomas Johann Seebeck Department of Electronics, TALLINN UNIVERSITY OF TECHNOLOGY, 2017, Tallinn, disponible en https://www.google.es/search?source=hp&ei=lAeDW-TqFtDVwQLVr4_ADg&q=JAMMING+OF+SPREAD+SPECTRUM+communications+use+in+uav+remote+control&oq=JAMMING+OF+SPREAD+SPECTRUM+communications+use+in+uav+remote+control&gs_l=psy-ab.3...1114.35170.0.36349.43.39.0.0.0.0.414.6607.0j19j10j1j1.31.0....0...1c.1.64.psy-ab..12.25.4921.0..0i22i30k1j33i22i29i30k1j33i160k1j33i21k1j33i10i21k1j33i10k1.0.OpRoOpS0R1Y

e) Gran número de drones 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

Los sistemas GNSS son sistema de navegación por satélite como el GPS[144] americano, GLONASS[145] ruso o el Galileo europeo. En el caso concreto del sistema GPS, se transmiten tres señales no-encriptadas (de uso civil y militar) y dos señales encriptadas (solo uso militar) sobre dos bandas diferentes denominadas L1 a 1575.42 MHz y L2 a 1227.6 MHz. Se está implementando una tercera señal civil denominada L5 a 1176.45 MHz[146]. El sistema Galileo emite en 4 bandas denominadas E1, E5a, E5b y E6. Ofreciendo un servicio abierto en las bandas E5a, E5b y E1, siendo las bandas E1 y E6 cifradas[147].

El *jamming* de las señales de los sistemas GNSS y en concreto del GPS es relativamente sencillo. La señal que emiten los satélites de posicionamiento es de baja potencia debido a la distancia a la que orbitan los satélites, por lo que el *jamming* no es excesivamente problemático tanto en señales encriptadas como no-encriptadas[148].

La pérdida de la señal GNSS para un dron puede suponer perder la habilidad de monitorizar su ruta, localización, altitud y dirección. Sin estos datos clave el dron puede verse incapacitado para realizar la misión[149].

Existen un gran número de dispositivos *jamming* fácilmente adquiribles por internet. Por ejemplo, se puede adquirir un dispositivo para conectar en un vehículo por menos de 5 euros y un rango de acción de hasta 15 metros[150].

---

[144] Del inglés *global positioning system*.
[145] Del ruso *global'naya navigatsionnaya sputnikovaya sistema*.
[146] HAY, Thomas E., «DETERMINING ELECTRONIC AND CYBER ATTACK RISK LEVEL FOR UNMANNED AIRCRAFT IN A CONTESTED ENVIRONMENT», AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY, August 2016, Alabama, disponible en http://www.dtic.mil/dtic/tr/fulltext/u2/1040702.pdf.
[147] https://m.esa.int/Our_Activities/Navigation/Galileo/What_is_Galileo
[148] «Técnicas de neutralización de amenazas aéreas basadas en el sistema de posicionamiento Galileo», Congreso sobre las Aplicaciones de los drones a la ingeniería civil, enero 2017, Madrid, disponible en https://www.civildron.com/pdf/civildron17-29_Tecnicas_de_neutralizacion_de_amenazas_aereas_basadas_en_el_sistema_de_posicionamiento_Galileo_AYESA_fenercom-2017.pdf
[149] MOROVITZ, Maretta, «Security Vulnerabilities in Unmanned Aircraft Systems», Department of Computer Science, Tufts University, December 2015, Medford, disponible en http://www.cs.tufts.edu/comp/116/archive/fall2015/mmorovitz.pdf
[150] https://www.ebay.es/itm/JAMMER-Anti-Tracker-GPS-Blocker-Car-Device-Cigarette-Lighter/283069860929?hash=item41e8474c41:g:PvMAAOSwuOpbVs6K

Capacidades

a) Son sistemas muy económicos y tecnológicamente sencillos.
b) Son altamente efectivos para drones que operan de manera autónoma, inhabilitando su guía u obligando al operador a tomar el control. Para drones 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[151]). Para el caso de los LSS UAS, una pérdida de señal válida de un sistema GNSS puede provocar la colisión contra el terreno o contra objetos colindantes.
c) Pueden ser direccionales u omnidireccionales, cubriendo grandes áreas. Por ejemplo, en el ejercicio Red Flag 18-1 se utilizaron aviones de guerra electrónica EA-18 *Growler* y EC-130 *Compass Call*, que interfirieron la señal GPS en una zona de 450 millas náuticas, unos 834 kilómetros[152].
d) Son altamente efectivos frente a enjambres de drones.
e) Al igual que las anteriores, son altamente flexibles, pudiéndose instalar en sitios fijos o móviles.

Limitaciones

a) Su empleo con sistemas omnidireccionales puede afectar a sistemas propios o no deseados.
b) Actualmente existe multitud de sistemas de navegación dual GNSS/inercial, de tal manera que si el dron 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 drones hostiles atacando objetivos de dimensiones moderadas.
c) Existen antenas con tecnología anti-*jamming* de GNSS como las ofertadas por la empresa Novatel[153] o la antena Small Antenna System (SAS) de la compañía Raytheon[154]. A su vez el Gobierno de Estados Unidos, a través de su Departamento

[151] DE WILDE, Wim, CUYPERS, Gert, SLEEWAEGEN, Jean-Marie, DEURLOO, Richard y BOUGARD, Bruno, «GNSS Interference in Unmanned Aerial Systems», Septentrio Satellite Navigation, Bélgica.
[152] https://arstechnica.com/information-technology/2018/02/dod-red-flag-exercise-ushers-in-gps-jamming-season-across-west/
[153] https://www.novatel.com/products/gnss-antennas/gajt-anti-jam-antennas/gajt/
[154] Para más información: https://www.raytheon.com/capabilities/products/gps_anti-jam

de Seguridad Nacional, desarrolló los programas *Patriot Watch, Patriot Shield y Patriot Sword*, para evitar la interferencia y uso ilícito del sistema GPS[155]. Por otro lado, hay numerosos programas que están desarrollando soluciones tecnológicas para evitar el *jamming* GNSS.

d) En el caso de zonas protegidas por *geofencing*[156], el interferir la señal GNSS del dron amenaza puede favorecer la entrada del dron en el área restringida.

e) La acción del *jamming* de la señal GNSS sobre un dron controlado por un operador puede no ser suficiente para neutralizarlo.

Ejemplos de sistemas de armas jamming

Los sistemas de armas *jamming,* debido a su precio y efectividad, están volviéndose muy populares[157]. Existen en el mercado sistemas de *jamming* exclusivamente de link de datos o de señal GNSS, pero los más demandados actualmente son los sistemas duales. Ejemplos de estos sistemas tenemos:

a) *DroneGun*: El DronGun es un fusil *jamming* montado sobre la base de un cuerpo del fusil AR-15. Este fusil va conectado por cable a una mochila que contiene el sistema de alimentación de corriente eléctrica así como el sistema de refrigeración. La distancia máxima de operación es 2 kilómetros y es capaz de realizar interferencias en las bandas 2.4 GHz ISM, 5.8 GHz ISM y opcionalmente las bandas GNSS L1 y L2. Su autonomía es de 1 hora de uso continuado (disponible de manera opcional baterías de 2 horas) y un tiempo de recarga de 4 horas[158].

[155] MOROVITZ, Maretta, «Security Vulnerabilities in Unmanned Aircraft Systems», Department of Computer Science, Tufts University, December 2015, Medford, disponible en http://www.cs.tufts.edu/comp/116/archive/fall2015/mmorovitz.pdf

[156] El *geofencing* es una barrera virtual geográfica, que se basa entre otros sistemas en el de posicionamiento GNSS para restringir la entrada de drones no autorizados. Muchos de los fabricantes de drones como DJI incluyen en sus sistemas estas restricciones. Para más información: https://www.heliguy.com/blog/2017/02/16/heliguys-guide-to-geofencing/

[157] En el documento Counter-Drone Systems de febrero de 2018 en el que se estudia el mercado de C-UAS actual, de un total de 151 sistemas analizados, 98 corresponderían a sistemas de armas *jamming*.

[158] Para más información: System Drone España S.R.L.

Figura 15: Fusil DroneGun. Fuente: https://www.unmannedairspace.info/counter-uas-systems-and-policies/droneshield-dronegun-certified-safe-radio-frequency-exposure/

b) *J4SKY-T Virtual-Fence*: Este sistema está formado por una red de antenas *jamming* de bajo coste para proteger grandes áreas como bases aéreas, aeropuerto o instalaciones críticas frente a la incursión de drones. Opera en una banda de trabajo desde 500 MHz hasta 3 GHz, siendo el *jamming* GPS opcional. Las antenas pueden ser omnidireccionales o sectoriales y, dependiendo del número de antenas, puede cubrir áreas de hasta 20 kilómetros y una altura de 1 kilómetro[159].

c) *AUDS Anti-UAV Defence System*: El AUDS es un sistema C-UAS de la compañía Bligther. Para la neutralización de amenazas dispone de un inhibidor de radiofrecuencia multibanda efectivo frente al link de mando y control y señal GNSS. El rango de interferencia va desde 400 MHz hasta 6 GHz. Las antenas son direccionales con un ancho de haz de 20 grados y un alcance máximo de 2 kilómetros[160].

[159] Ibíd.
[160] Para más información: http://www.blighter.com/products/auds-anti-uav-defence-system.html

Figura 16. Sistema AUDS. Fuente: https://www.flickr.com/photos/blighter-surveillance-systems/34532680535/in/album-72157649675559583/

d) *R-330ZH*: El R-330ZH es un sistema *jamming* de fabricación rusa capaz de interferir sobre sistemas de comunicación vía satélite, comunicaciones GSM-1800 y señales GNSS. Puede interferir las bandas de 100 MHz a 2.000 MHz. Su alcance sobre objetivos aéreos es superior a 200 kilómetros. Durante el ejercicio Union Shield 2015 en Bielorrusia este sistema fue utilizado para neutralizar drones[161].

e) *Otros*: Existen multitud de sistemas de *jamming* no diseñados específicamente para amenaza UAS, capaces de interferir en las bandas de operación de estos. Ejemplos vistos anteriormente como el EG-18 Growler o el EC-130 Compass Call, que vienen de desarrollos rusos como el avión de guerra electrónica IL-22P o sistemas como el Borisoglebsk-2[162].

Operaciones en el ciberespacio (Cyber)

Con anterioridad se definió el concepto de ciberespacio y las consideraciones de las operaciones en este dominio sintético.

[161] MCDERMOTT, Roger N., «Russia´s Electronic warfare Capablities to 2025, Challenging NATO in the electromagnetic spectrum», International Centre for Defence and Security, September 2017, disponible en https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

[162] Ibíd.

La concepción tradicional de la ciberdefensa es la de garantizar el acceso al ciberespacio y la de proteger los sistemas de información y de telecomunicaciones, así como asegurar la disponibilidad, integridad y confidencialidad de la información de interés. En el caso particular de España, y a través del Mando Conjunto de Ciberdefensa, en su cometido número cinco: «Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional, este Mando puede ejercer dicha labor aplicada a la defensa del espacio aéreo»[163].

La ciberdefensa del espacio aéreo no solo implica la protección del SDA de ciberamenazas, implica formar parte del SDA como un actor más desde el punto de vista defensivo y, a su vez, de una manera ofensiva, pudiendo ser un elemento más de neutralización de amenazas aéreas. Un dron es esencialmente una computadora volante, por lo que es susceptible a ciberataques.

Ciberataque a drones

Los sistemas aéreos no tripulados están compuestos principalmente por dos segmentos: El segmento aéreo y el segmento terrestre. El segmento aéreo lo forman la plataforma aérea y sus subsistemas y el segmento terrestre la estación de control terrestre o GCS[164] como muestra la tabla 6.

[163] http://www.emad.mde.es/CIBERDEFENSA/cometidos/

[164] Del inglés *ground control system.*

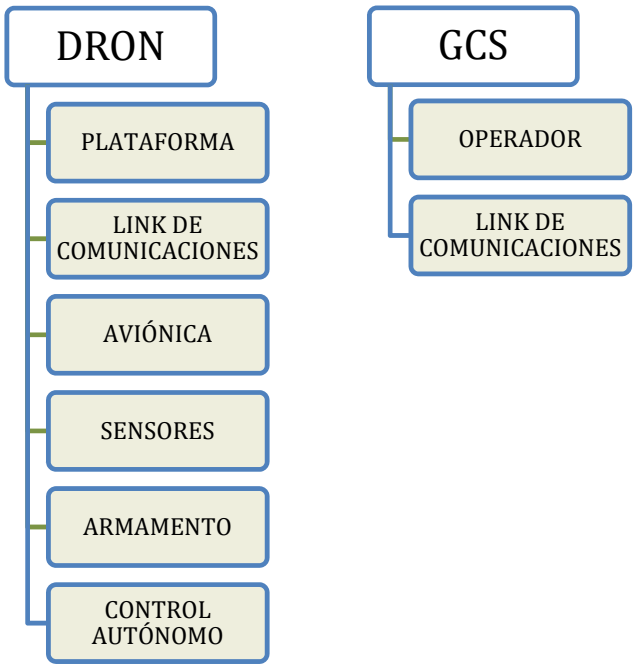

Tabla 6: Componentes de un sistema aéreo no tripulado. Fuente: https://ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdf

Ambos segmentos son vulnerables a los ciberataques, desde la comunicación interna de sus subsistemas a la comunicación externa de la cual son altamente dependientes ambos segmentos, así como del flujo de información del entorno hacia los sensores[165].

Existen diversos tipos de ciberataques en función del segmento o subsistema sobre el que se desee actuar. Entre estos destacan[166]:

- Ataque remoto: Es un ataque que se realiza a través de uno de los sensores o canales de comunicación.
- Ataque sobre el hardware: El ataque se realiza directamente sobre los componentes tras acceder a los mismos.

Otros tipos de ataques más específicos son:

- Ataque sobre el sistema de mando y control de la carga de pago: En este tipo de ataque se accede a la información que transmite alguno de los sistemas del dron.

[165] HARTMANN, Kim y STEUP Christoph, «The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment», 5th International Conference on Cyber Conflict, 2013, Tallinn, disponible en https://ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdf

[166] SAMSÓ, Laura, «CYBERWAR Hacking Drones. Cyberspace & Interconnected Systems», October Atlanta, disponible en http://www.centuriontechnologies-llc.com/wp-content/uploads/2017/10/HH_drones_cybersecurity_3.pdf

- Ataque directo a la carga de pago: Este tipo de ataque inhabilita o destruye la carga de pago (sensores EO[167], IR, LIDAR[168]…).
- Ataque al sistema de control: Se ataca el *software* o *hardware* del sistema de control del dron. Evita que el *software*, *hardware* o la CPU se comporten según está programado.
- Ataque a la lógica de las aplicaciones: Altera los datos del sistema de control. Se manipulan los datos de los sensores o del entorno para proporcionar datos falsos[169].
- Los ciberataques más comunes son el *spoofing* de la señal GNSS y el «hackeo» para interceptación de datos o secuestro del dron.

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 GNSS proporcionándole información falsa de posición, velocidad y tiempo (PVT). 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[170]. Existen diversos tipos de ataques *spoofing* como *True-signal nulling o el Multi-transmitter*.

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 rerradiarlas posteriormente. Si el receptor interpreta estas señales como válidas, estará asumiendo un error[171].

[167] Del inglés *electro optical.*
[168] Del inglés *light detection and ranging.*
[169] SAMSÓ, Laura, «CYBERWAR Hacking Drones. Cyberspace & Interconnected Systems», October Atlanta, disponible en http://www.centuriontechnologies-llc.com/wp-content/uploads/2017/10/HH_drones_cybersecurity_3.pdf
[170] RÜGMAMER, Alexander y KOWALEWSKI, Dirk, «Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!», FIG Working Week 2015, May 2015, Sofia, Bulgaria, disponible en https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf
[171] Ibíd.

Capacidades

a) Son un tipo de ataque muy económico y tecnológicamente sencillo.
b) Son altamente efectivos para drones que operan de manera autónoma con sistema GNSS no encriptado.
c) Son accesibles tanto en el mercado civil como el militar[172].
d) Pueden permitir el control y captura de un dron o su destrucción, guiando al mismo a un área de control o haciéndole volar a un lugar donde colisione.
e) Pueden pasar inadvertidos para el enemigo, de tal manera que no sepa que sus drones estén siendo atacados con sistemas de *spoofing*.

Limitaciones

a) Su empleo con sistemas omnidireccionales puede afectar a sistemas propios o no deseados.
b) Necesita de operadores con conocimientos avanzados a diferencia de otros sistemas de armas no cinéticos.
c) Frente a señales GNSS encriptadas sus efectos son limitados. Para estos casos se puede emplear *Meaconing*.
d) Existen numerosos desarrollos tecnológicos para detectar ataques *spoofing*.
e) La acción del *spoofing* de la señal GNSS sobre un dron controlado por un operador puede no ser suficiente para neutralizarlo.
f) En el caso de un ataque por enjambre y una sola antena para *spoofing* disponible, la señal enviada será similar para todos los drones del enjambre independientemente de su posición, por lo que es necesario un estudio situacional para evitar que alguno de los drones se dirija al lugar a proteger[173].
g) Su alcance es limitado.

Hackeo para interceptación de datos o secuestro de dron

Como se vio anteriormente, tanto drones como estaciones en tierra (GCS) son susceptibles a ciberataques en sus diferentes segmentos o subsistemas. Entre los

[172] Existen desarrollos comerciales como el SimSAFE o el Spirent.
[173] LÓPEZ, Patricia, MUÑOZ, Alejandro, ARCE, Alicia y GALÁN, Ricardo, «Efectos de la suplantación de señales GNSS sobre una flota de UAV y su aplicación a la defensa de áreas restringidas», Fundación Ayesa, 2018, disponible en https://www.fundacionayesa.org/wp-content/uploads/2018/03/CivilDron18_Spoofing.pdf

ataques más comunes destacan la exposición a virus informáticos de los GCS, ataque sobre el link de comunicaciones entre dron y GCS o ataque al sistema operativo propio del dron[174]. Por ejemplo, el Maldrone es uno del software más generalizado. Puede ser instalado en cualquier ordenador que sea capaz de conectarse a la red Wifi o a otro dron e insertar un archivo malicioso. Una vez insertado el archivo intercepta las señales entre dron y su controlador pudiendo tomar el control del mismo[175].

Capacidades

a) Son un tipo de ataque muy económico.
b) Son altamente efectivos para drones no protegidos frente a ciberataques.
c) Pueden permitir el acceso a información de sensores, control o destrucción del dron.
d) Pueden pasar inadvertidos para el enemigo.

Limitaciones

a) Necesita de operadores altamente especializados y con amplios conocimientos de la plataforma a atacar.
b) Ante drones protegidos frente a ciberataques su acción puede ser extremadamente compleja.
c) Existen numerosos desarrollos tecnológicos para protegerse frente a ciberataques, como sistemas de comunicaciones encriptadas, cortafuegos...

Ejemplo de ataques

a) En 2011 el Ejército americano perdió un dron RQ-170 Sentinel que realizaba una misión en espacio aéreo iraní. Irán confirmó que estaba en posesión del citado dron. Se cree que el dron fue capturado mediante un ataque combinado de *jamming* a su link de datos satélite junto con *spoofing* de GPS, consiguiendo capturar el dron y hacerlo aterrizar en una base iraní[176].

[174] HARTMANN, Kim y STEUP Christoph, «The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment», 5th International Conference on Cyber Conflict, 2013, Tallinn, disponible en https://ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdf
[175] TRUJANO, Fernando, CHAN, Benjamin, BEAMS, Greg y RIVERA, Reece, «Security Analysis of DJI Phantom 3 Standard», May 2016, disponible en https://courses.csail.mit.edu/6.857/2016/files/9.pdf
[176] HARTMANN, Kim y STEUP Christoph, «The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment», 5th International Conference on Cyber Conflict, 2013, Tallinn, disponible en https://ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdfNOTICIAS EN PRENSA.

Figura 17. Supuesta copia iraní del dron RQ-170. Fuente: http://time.com/3575809/iran-american-drone-first-flight/

b) En diciembre de 2015, el Departamento de Seguridad Nacional (DHS[177]) de los Estados Unidos declaró ser víctima de ataques *spoofing* y *jamming* en su flota de drones para patrulla fronteriza. Los citados ataques se atribuyen a los cárteles de droga, en un intento de evadir el control de los citados drones[178].
c) En 2009, insurgentes iraquíes hackearon drones Predator utilizando el software comercial SkyGrabber de creación rusa. Los insurgentes tuvieron acceso a las imágenes enviadas por el dron, atacando su link de datos no encriptado[179].
d) Casos similares se han reportado sobre drones israelitas por parte de grupos terroristas palestinos[180].
e) El SkyJack de Samy Kamkar, es un dron diseñado para buscar de forma autónoma, hackear y controlar de forma inalámbrica otros drones a una distancia Wifi, creando un ejército de drones zombis bajo su control. El autor explica en un tutorial como crear tu propio dron hacker de una manera sencilla y económica[181].

[177] Del inglés *department of homeland security*.
[178]https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/
[179] http://edition.cnn.com/2009/US/12/17/drone.video.hacked/index.html
[180] https://www.thedailybeast.com/how-islamic-jihad-hacked-israels-drones
[181] http://samy.pl/skyjack/

Comparativa cinético contra no-cinético

Con anterioridad se han enumerado una serie de limitaciones de los sistemas de armas cinéticos frente a los VANT y, a su vez, se han introducido nuevos sistemas de armas no cinéticos junto con sus ventajas y limitaciones. Realizando una comparativa entre ellos podemos concluir que los sistemas no cinéticos mejoran ostensiblemente en campos como el daño colateral, economía, cantidad, efectividad y eficiencia. Por otro lado, los sistemas no cinéticos presentan carencias frente a los cinéticos como el alcance, la letalidad o el riesgo de fratricidio en algunos casos. A su vez, muchos de estos sistemas de armas son sistemas en desarrollo, por lo que su tecnología está en proceso de implementación, aunque existen lagunas doctrinales y necesidad de tácticas, técnicas y procedimientos (TTP), al igual que los sistemas de armas cinéticos.

No existe una solución única para la amenaza dron. La solución pasa por una concepción híbrida de sistemas de armas cinéticos y no cinéticos donde se complemente y se cubran mutuamente las carencias identificadas. Ante una amenaza híbrida se deben aplicar soluciones híbridas.

El ataque con drones sobre bases rusas en Siria

El día 8 de enero de 2018, la base aérea de Hmeymin y las instalaciones navales de Tartus, ambas operadas por fuerzas rusas, sufrieron un ataque masivo y coordinado con drones. Los drones, realizados de manera artesanal, tenían sistema de navegación GPS y portaban 5 bombas caseras de 400 gramos con explosivo PETN[182]. En total se neutralizaron 13 drones, 10 de los cuales atacaron la base aérea y 3 las instalaciones navales. El método de neutralización llevado a cabo por las fuerzas rusas consistió en una acción combinada de sistemas de armas cinéticos y no cinéticos. El sistema Pantsir-S derribó 7 de los drones, mientras que los otros 6 fueron neutralizados con un sistema de armas no cinético, consiguiendo que de esos 6 drones 3 sobrevivieran al aterrizaje. Posteriores análisis de los drones capturados indicaron que siguieron una trayectoria de vuelo de en torno a 50 kilómetros, teniendo como zona de despegue la ciudad de Muzawarra, siendo estos capaces de recorrer hasta 100 kilómetros[183].

[182] Acrónimo de tetranitrato de pentaeritritol, también conocido como pentrita. Es uno de los explosivos más potentes conocidos, con un factor de efectividad relativa de 1,66. Para más información: https://es.wikipedia.org/wiki/Pent

[183] https://www.uasvision.com/2018/01/12/details-of-drones-that-attacked-russias-syrian-bases/

Sobre este ataque diversos especialistas como Denis Fedutinov coinciden en que un dron armado de bajo coste y de estas características empleado en forma de enjambre puede suponer una verdadera amenaza. A su vez, las armas de defensa aérea tradicionales no siempre son lo suficientemente efectivas, por la dificultad que supone enfrentarse a esta amenaza y por la relación de coste amenaza frente a arma defensiva. Es por ello que los sistemas electrónicos jugarán un rol primordial en el futuro[184].

El ataque anterior podríamos identificarlo como el germen de las futuras amenazas *swarm*.

Figura 18. Detalle dron artesanal capturado y su munición. Fuente: https://www.timesofisrael.com/russian-military-shows-drones-it-says-came-from-syria-raid/

Otras consideraciones:

Aproximación holística

El fenómeno dron y las implicaciones que está generando en términos de seguridad debe ser acometido de una manera holística. Este fenómeno afecta no solo a las Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado, sino que implica a toda la

[184] Ibíd.

sociedad. Es por ello que debe ser tratado desde un punto de vista multidisciplinar e interministerial.

Multidominio y estrategia conjunta

Los ejércitos y la Armada operan mayoritariamente en el dominio bajo su responsabilidad. Los continuos desarrollos doctrinales para la acción conjunta han favorecido las acciones coordinadas en los distintos dominios y la unidad de acción. Las nuevas tecnologías en el ámbito cibernético y de los sistemas no tripulados o autónomos hacen necesario un nuevo avance doctrinal. Los drones aéreos se han convertido en multiplicadores de la fuerza y su uso no es exclusivo de las fuerzas aéreas, por lo que cada vez existen más usuarios del dominio aéreo. En este contexto son necesarias mejores y mayores formas de coordinación y operación, tanto de carácter defensivo como ofensivo. En este sentido se está desarrollando el denominado multidominio[185], algo que será clave en las operaciones futuras para la defensa antidrón.

Mando centralizado, ejecución descentralizada

Esta es una de las máximas para la defensa aérea. La magnitud de la amenaza dron y en concreto de los LSS UAS, requiere una aproximación holística como se vio anteriormente. Es por ello por lo que es necesario un mando centralizado que coordine las acciones o asigne responsabilidades a cada uno de los responsables de la defensa, civiles o militares, en tiempo de paz, conflicto o guerra. En el caso particular de España, el responsable de la defensa del espacio aéreo es el Ejército del Aire y es este el que debe establecer las directrices con el resto de actores (FCSE, CNPIC[186], otros ministerios…) para una defensa eficaz, optimizada e interoperable con los recursos disponibles. En este sentido, dentro del Departamento de Seguridad Nacional (DSN)[187] podría evaluarse la necesidad de un Comité Especializado en sistemas no tripulados o autónomos.

[185] Para más información sobre este concepto: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/Perkins-batalla-multidominio-1.pdf
[186] Acrónimo de Centro Nacional de Protección de Infraestructuras y Ciberseguridad.
[187] Para más información sobre el DSN: http://www.dsn.gob.es/es

Interoperabilidad y movilidad

La amenaza dron afecta tanto al dominio aéreo como al terrestre, marítimo y cibernético. Para contrarrestar este tipo de amenaza son necesarios más instrumentos que los aportados por el SDA debido a sus especiales características, vistas con anterioridad. Es por ello que esta amenaza debe ser acometida de una manera global. En la acción global la interoperabilidad es la clave, ya que favorece la unidad de acción, ahorra costes y aumenta la efectividad.

Por otro lado, esta amenaza puede ser extremadamente móvil y volátil, por lo que la movilidad propia debe ser una máxima para enfrentarse en igualdad de condiciones.

Defensa pasiva

Las características de la amenaza dron hacen difícil contrarrestarla con los sistemas actuales. Siendo una amenaza tan móvil y numerosa, la adquisición de sistemas de armas para intentar neutralizarla puede conllevar costes inasumibles para una nación. Las defensas pasivas, en concreto frente a amenazas LSS UAS con un poder destructivo más discreto, pueden ser útiles, efectivas y disuasorias. Medidas como establecer un programa nacional de *geofencing* para instalaciones consideradas de interés, bunkerización de instalaciones vulnerables, uso de redes antidrón o un mayor control en la adquisición de estos artefactos pueden ser opciones alternativas al despliegue de costosos sistemas de armas.

Importancia del espectro electromagnético

Conforme evoluciona la tecnología aumenta la dependencia de esta del espectro electromagnético. El control del espectro electromagnético es vital para la defensa de los intereses nacionales y específicamente para el control del dominio aéreo frente a la amenaza dron. No se puede destruir algo que no se puede identificar, no se puede destruir algo que no se puede detectar, no se puede destruir algo sobre lo que no se puede informar, la balanza entre cinético no-cinético debe compensarse, ya que el futuro pasa por el control del espectro EM.

Acelerar los ciclos

Es imposible alcanzar a algo que se desplaza más rápido que uno mismo. Por norma general las estrategias defensivas suelen ser reactivas, es decir, se crean las medidas

cuando se sufre una acción. El ritmo de los avances tecnológicos actuales y las tecnologías de doble uso hacen plantearse un cambio de estrategia en la forma de enfrentarse a las nuevas amenazas, este cambio debe orientarse hacia estrategias proactivas donde se identifiquen las posibles amenazas antes de que se produzcan. Para ello es muy importante una nueva visión doctrinal, donde se adapten los ciclos estratégicos, operacionales y tácticos a las nuevas amenazas no convencionales como los drones.

Human in the loop (HITL)

El HITL se define como cualquier modelo que requiere la interacción humana. Como hemos visto durante este documento, existen drones que no requieren de la interacción humana y a muy corto plazo los ejércitos de drones autónomos (*swarm*) verán la luz. Actualmente en la gran mayoría de sistema de defensivos u ofensivos el HITL está presente al menos para los casos de neutralización, asignando a los sistemas autónomos labores que no impliquen la destrucción. Con los nuevos avances tecnológicos en campos como la inteligencia artificial, mantener el HITL como autoridad para la neutralización puede ser una limitación que puede poner en peligro la propia autodefensa. Los sistemas de armas no cinéticos vistos con anterioridad, debido a sus especiales características como el reducido daño colateral, pueden ser candidatos para eliminar el HITL del proceso de toma de decisiones, confiriendo autonomía bajo ciertos supuestos como una acción máquina contra máquina.

Por ejemplo, el tiempo empleado por un dron de tipo 2, cargado de explosivos, en un ataque suicida autónomo frente al tiempo de reacción de un sistema de defensa al aplicar los procesos de detección, identificación y neutralización, junto a la demora producida por la acción del HITL, puede ser tal que sea imposible su neutralización en multitud de casos. En este supuesto el elemento débil de la cadena es el hombre, por lo que eliminar a este para los casos máquina contra máquina, en los que no se ponen en peligro vidas humanas de manera directa, debe tomarse en consideración para futuros escenarios.

La eterna espera

La tecnología aplicada a los sistemas de armas no cinéticos como la tecnología láser o HPM está en un proceso continuo de desarrollo, favorecida por sus aplicaciones de doble uso. Esta mejora continua hace que sea difícil definir las especificaciones técnicas

requeridas a un sistema de armas o se decida paralizar la adquisición a expensas de mejoras significativas en breve espacio de tiempo[188]. Esta situación hace que la introducción de estos sistemas de armas se vaya demorando y se dé un proceso de eterna espera. Una forma de paliar este problema es recurrir a tecnología modular, uso de tecnología civil que abarate costes e inversión en industria nacional que repercuta en la propia nación.

Conclusión

Los vehículos aéreos no tripulados y más concretamente los LSS UAS suponen un riesgo creciente para la defensa aérea. Los Sistemas de Defensa Aérea actuales y sus sistemas de armas cinéticos para la neutralización de amenazas están basados en una concepción doctrinal frente a amenazas tradicionales que debe ser actualizada. La solución a esta amenaza no pasa por sustituir el concepto actual de la defensa, sino complementarlo a la nueva amenaza dron y cubrir las carencias identificadas. Entre las carencias más importantes están la económica, la material y el daño colateral. Los sistemas de armas no-cinéticos cubren parte de estas carencias, por lo que son el complemento a integrar en los SDA. La balanza cinético y no-cinético en los próximos años debe equilibrarse ya que las nuevas amenazas son más dependientes del espectro electromagnético, por lo que debe actuarse en consecuencia. La pregunta que debe hacerse no es si integrar o no sistemas de armas no-cinéticos para la defensa aérea, la pregunta es el cuándo, ya que la defensa aérea no puede prescindir de estos sistemas de armas.

*José Alberto Marín Delgado**
Capitán del Ejército del Aire
Piloto de combate

[188] PUDO, Dominik y GALUGA, Jake, «High Energy Laser Weapon Systems: Evolution, Analysis and Perspectives», Canadian Military Journal, summer 2017, disponible en http://www.journal.forces.gc.ca/Vol17/no3/PDF/CMJ173Ep53.pdf