PRESENTE Y FUTURO DE LOS DRONES COMERCIALES LETALIZADOS

Juan Luis CHULILLA CANO
CEO, Red Team Shield, Ltd.

Introducción

OS que peinamos canas recordamos la acepción de dron como blanco aéreo. De sistemas completamente específicos, hemos pasado a un término conceptualmente más amplio que cualquier otro sistema militar. En 2023 se denomina dron a un *Black Hornet* (o a su equivalente civil, menos capaz pero no despreciable, un *Tiny Whoop*), a un *Global Hawk* y a todos los sistemas entre medias. También, para desgracia general, hemos evolucionado de una situación en la que muy pocas fuerzas armadas disponían de drones armados a un momento en el que han llegado a manos de actores no estatales hostiles.

El dron comercial letalizado (1) reduce el concepto a un ámbito más manejable. Se trata de productos de menos de 25 kg (aún más ligeros en la mayoría de los casos), diseñados y producidos fuera de la industria de defensa o aeronáutica, y que pueden ser adquiridos o incluso fabricados por pequeños grupos civiles o individuos aislados.

El principal obstáculo cultural es el de *juguete*: el tamaño, el aspecto y su presencia en los lineales de los supermercados trabaja en nuestra contra y,

(1) El término dron comercial letalizado ha sido acuñado por el autor del presente artículo y se publicó por primera vez en «Letalización de drones comerciales». *Estrategia podcast 49*. *https://youtu.be/7MyeFE-j9W8*

pese al extenso historial de eventos letales protagonizados por ellos, la amenaza no ha sido abordada en tiempo y forma, tanto porque no se ha materializado en nuestro territorio europeo, como porque un juguete no es peligroso. Como prologaba el secretario de Defensa Miller (2):

Challenges to the Joint Force are more complex and varied than at any other time. Rapid technological change has aided in disrupting the international rules-based order. Small unmanned aircraft systems (sUAS) were previously viewed as hobbyist toys, but today it is evident that the potential for hazards or threats has the ability to impact the Joint Force.

Finalmente, dentro de los drones comerciales letalizados hay una distinción esencial: por una parte, tenemos los productos *privativos* de empresas tales como DJI, Autel, Parrot, etc., de capacidades cada vez más avanzadas y orientados a un uso simplificado. Por otra, están los artículos de *autofabricación* a partir de componentes libres, que veremos de inmediato. En este caso, la barrera de entrada es más elevada, pero a cambio la adaptabilidad es básicamente ilimitada.

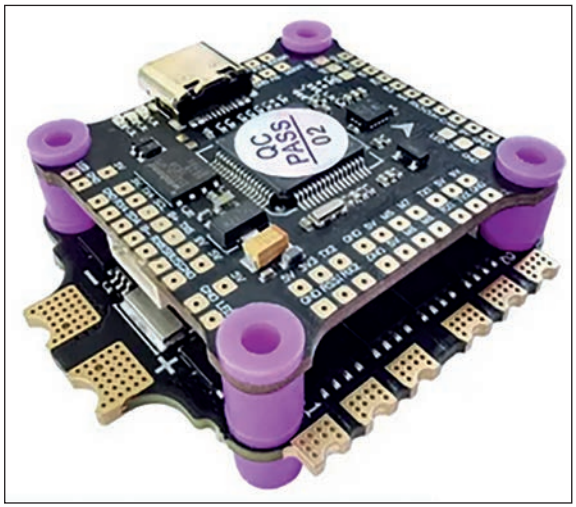
Cómo hemos llegado hasta aquí

En una sola palabra: *smartphones* o incluso los mandos de las consolas Wii (3). A partir de 2013 se superaron los mil millones de unidades vendidas al año, hasta alcanzar la meseta de los mil quinientos millones. Semejante explosión tecnológica tuvo como consecuencia, entre otras, que componentes digitales tales como giroscopios, acelerómetros o barómetros alcanzaran en muy poco tiempo la excelencia, tanto en precisión como en precio. Aunque éstos no logren la fiabilidad y especificación de sus equivalentes aeronáuticos o militares, ofrecen resultados satisfactorios a un coste reducido en cuatro e incluso más órdenes de magnitud. Por ejemplo, una controladora de vuelo Matek F722 encaja en una placa de 36 x 46 mm una CPU ARM STM32 optimizada para operaciones en tiempo real, giroscopio, acelerómetro, barómetro, caja negra para telemetría y multitud de puertos para la comunicación con otros componentes. Incluso después de los problemas de suministro chinos, esta placa cuesta 45,96 euros.

---

(2) MILLER, C. C. (2021): *Counter-Small Unmanned Aircraft Systems Strategy*. US Department of Defense.https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF

(3) SPYCHALSKI, P. (2020): «A brief history of a flight controller. From MultiWii to Betaflight and beyond». *QuadMeUp. https://quadmeup.com/a-brief-history-of-a-flight-controller-from-multiwii-to-betaflight-and-beyond/*



Controladora de vuelo Matek F722.
(Fuente: Matek Systems)

Dos palabras más complementan a *smartphone*: *open source*. Ebeid *et al*. (4) resumen la última década de evolución de *hardwares* y *softwares* libres aplicados a los sUAS. Por una parte, la totalidad de los sistemas operativos (*firmware*) empleados en controladoras son de licencia libre y están basados en proyectos comunitarios. El *firmware* traduce en tiempo real las órdenes que envía el piloto a través de su emisora de radio (o las que tiene almacenadas en su programación) en instrucciones para las superficies de control (caso de un avión) o del giro de los motores de un *quadcopter*. Este último caso es en especial, relevante debido a que es humanamente imposible mantener bajo control un sUAS aumentando o disminuyendo la velocidad de cada uno de sus cuatro motores por separado.

Por otro lado, la importancia del *hardware* libre ha sido capital: el acceso a la totalidad de los elementos de diseño de forma legal y gratuita ha permitido que muchísimos fabricantes ofrezcan controladoras muy capaces y las hagan evolucionar en ciclos extremadamente cortos.

Componentes tan eficaces como económicos en manos de *comunidades de práctica* que trabajan en un ambiente competitivo se han combinado para ofrecer a individuos talentosos y persistentes la totalidad de los recursos necesarios para construir, programar y poner en vuelo aparatos inconcebibles hace no muchos años, tanto en precio como, sobre todo, en capacidades. Y, por supuesto, son capacidades estrictamente neutras: el piloto deportivo y el *maker,* que desarrollan sus habilidades de forma pacífica y legítima, utilizan los mismos recursos que el actor hostil cuando letaliza estos aparatos.

(4) Ebeid, *et al*. (2018): «A survey of open-source UAV flight controllers and flight simulators». *Microprocessors and Microsystems*, *61*, pp. 11-20 *https://www.sciencedirect.com/science/article/abs/pii/S0141933118300930*

Pilotos en una competición de sUAV. (Fotografía facilitada por el autor)

Grupo de voluntarios de Aerorózvidka manipulando un dron *R-18* con dos granadas. (Fotografía facilitada por el autor)

Estado del arte

El problema de partida: la variedad de componentes es tal que dificulta sobremanera la modelización de todas las posibilidades significativas para estos drones comerciales. Por tanto, en aras de la brevedad, se mencionarán los componentes más críticos para comprender las capacidades de los drones comerciales letalizados.

En primer lugar, la plena madurez de las baterías de litio (tanto las de polímero como las de ion) ofrece alcances, cargas y velocidades notables a aparatos pequeños y de coste modesto. Otros componentes esenciales ayudan a concebir a los sUAS de dos formas presentes y una futura. Éstas son:

1. Es una *radio que vuela*. Un sUAS sigue siendo un sistema que emite información y recibe comandos. El sUAS actual está muy limitado, sin un *man-on-the-loop* al que remitirle información (vídeo, telemetría) y de quien recibir instrucciones. Las frecuencias y protocolos han evolucionado significativamente en la última media década y, por lo tanto, su contramedida tiene que cubrir muchos más escenarios que en 2015. Además, la modificación de las emisoras para aumentar la potencia de emisión tiene una barrera de entrada baja para los que quieran superar las barreras legales.
2. Es una *cámara que vuela*. Tanto para pilotaje (si es el caso), como para ISR (inteligencia, vigilancia y reconocimiento) y designación de blanco, la cámara de vídeo que emite a la base y graba internamente ha aprovechado la explosiva evolución de las cámaras para *smartphones*. En la actualidad, un presupuesto económico da acceso a cámaras de baja luminosidad e incluso a cámaras térmicas plenamente operativas. El *feed* de vídeo puede recibirse a kilómetros (hasta 30 con algunos videotransmisores, VTX) o ser procesado en diferido.
3. Será una *unidad de procesamiento de tensores o neuronal (TPU/NPU) que vuele*. Una TPU/NPU ofrece amplísimas y preocupantes posibilidades para los diseños de mañana, literalmente. Si algunos productos comerciales avanzados ya son capaces de seguir a un blanco a velocidad moderada a través de bosques, a corto plazo esa capacidad se va a expandir y a generalizar, y con ello los drones comerciales letalizados tendrán la opción de prescindir de piloto e incluso de GNSS (sistema global de navegación por satélite).

Apuntes para la historia de la letalización de los drones comerciales

Antes de Ucrania

Por más que haya antecedentes (intentos de la Baader-Meinhof, 1977, o de Aum Shinrikyo, 1994), en general se acepta que la primera letalización

sistemática de los drones comerciales tiene lugar en los distintos escenarios de Oriente Próximo a partir de 2013 (5) (6). Anteriormente a esa fecha, distintos cuellos de botella tecnológicos no permitían la viabilidad del sUAS como vector letalizado efectivo. Algunos grupos comenzaron a importar *quadcopters*, y las circunstancias del conflicto se combinaron con el estado del arte drónico de esos años para alcanzar un ritmo de innovación que entonces parecía vertiginoso y ahora resulta comparativamente lento. Con todo, el cambio principal es disruptivo y profundo: de ser víctimas de los ataques con drones, los actores no estatales pasaron a emplearlos.

En aquellos días, ni el *software* ni el *hardware* eran *libres* (lo que dificultaba su modificación y evolución), ni los conocimientos estaban suficientemente *diseminados*. De hecho, la primera serie de sUAS comerciales realmente exitosa, los *Phantom* de la empresa DJI, llevaban poco más de un año en el mercado. Se trataba de aparatos muy lentos, de tamaño, peso y volumen muy superiores a los actuales (el primero no empleaba baterías Li-Ion, sino de NiMh), pero que aportaron capacidades inéditas. A éstas se le unía el precio: por menos de 1.000 euros se podía acceder a un aparato que se mantenía en el aire más de 20 minutos y que podía operar y transmitir vídeo a unos cuantos miles de metros de distancia. En poco tiempo, su rol de ISR se amplió a otros más letales. Ya entonces se advertía:

What's most concerning is that the majority of the innovation in this field has been achieved by the enemy in a warzone. This is both an amazing achievement and a horrific one that is a harbinger of things to come. Meanwhile it seems… that the Pentagon is in denial of just what this all means for the future of warfare and quite frankly, humanity (7).

La ingeniería inversa sobre el *firmware* de los drones comerciales privativos ha permitido superar sus límites de fábrica: sus trayectorias no estarán limitadas por *software* (*geofencing*), de manera que podrán entrar en espacios prohibidos; de igual forma, dejan de ser vulnerables para Aeroscope (8), con lo que las Fuerzas y Cuerpos de Seguridad del Estado ya no pueden tomar el

---

(5) BUNKER, R. J. (2015): «Terrorist and insurgent unmanned aerial vehicles: use, potentials, and military implications». *Strategic Studies Institute*, US Army War College. *https://scholarship.claremont.edu/cgi/viewcontent.cgi?article=1050&context=cgu_facbooks*

(6) CHÁVEZ, K.; SWED, O. (2020a): « Off the shelf: the violent nonstate actor drone threat». *Air and Space Power Journal*, 29, *https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf*

(7) ROGOWAY, T. (2017): *«ISIS drone dropping bomblet on Abrams Tank is a sign of what's to come». The War Zone, http://twitter.com/thewarzonewire/status/824752127922679808*

(8) Aeroscope, de la marca comercial DJI, es un sistema de detección de drones que permite al usuario rastrear los datos volcados por la telemetría de los drones fabricados por DJI en un espacio aéreo de un radio de 5 a 20 kilómetros.

control del aparato y localizar al piloto como con Aeroscope en funcionamiento. Modificaciones adicionales han llegado a incluir sistemas de lanzamiento de granadas.

El conflicto civil sirio no fue sólo la cuna de la letalización del dron comercial: fue también donde se emplearon estos vectores con más profusión y efecto. Hasta la guerra de Ucrania, claro.

Ucrania: punto de inflexión

En febrero de 2014, las Fuerzas Armadas de Ucrania padecían una severa serie de carencias. Una de ellas era la de sUAS como recurso táctico de ISR. Algunos grupos voluntarios se encargaron de la tarea. Tucker (9) los denomina *war startups*, debido a su cultura y sus ciclos de desarrollo. Sin embargo, conviene considerar también el papel horizontal y autoorganizativo de los grupos informales del Euromaidán (10). Las mismas redes de personas se volcaron en apoyar a los combatientes de un ejército con graves carencias o incluso en unirse al combate en pequeñas unidades voluntarias. Una de las formas de ayudar fue aportar recursos de ISR basados en drones comerciales.

Enfrente tenían a un adversario con abundantes recursos en guerra electrónica (EW), que les limitaba y que tuvieron que aprender a sortear. El portavoz del grupo Aerorózvidka (11) explica la dureza de ese proceso de aprendizaje y el precio de los errores.

El concepto de *juguete* siguió jugando en contra de las Fuerzas Armadas ucranianas (ZSU). Pese a las ventajas demostradas por los sUAS, las ZSU mantuvieron los drones comerciales en manos de los voluntarios y se centraron en los modelos militares de fabricación local o importada. Cuando el 24 de febrero de 2022 el conflicto adquiere un carácter existencial, fueron los voluntarios los que tuvieron que volver a dar un paso al frente. Algunos ejemplos: Aerorózvidka (12) ha desarrollado dos proyectos capitales para el esfuerzo de guerra: el dron letalizado *R-18* (con su cargamento de granadas anticarro) y el

(9) Tucker, P. (2015): «In Ukraine, Tomorrow's Drone War Is Alive Today». *Defense One*, 3 de marzo de 2015. *https://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/*

(10) Onuch, O. (2015): «EuroMaidan protests in Ukraine: Social media versus social networks». *Problems of Post-Communism*, *62*(4), pp. 217-235.

(11) Aerorózvidka es una ONG formada por voluntarios ucranianos que han puesto sus conocimientos y recursos en materia de sUAV y ciberdefensa a disposición de las Fuerzas Armadas de Ucrania.

(12) Chulilla, *et al*. (2022): entrevista al portavoz de Aerorózvidka, *https://youtu.be/5F7qFDzvYqU*

BMS DELTA. Drone Labs (13) ha modificado drones de autofabricación para aumentar su grado de supervivencia frente a sistemas EW rusos, como el Krasukha-5; su líder, Maxim Sheremev, llama *flying microwave ovens* a sus *quads*. Por su parte, Army SOS (14) ha encontrado en el uso de sUAS de ala fija y autónomos los mejores resultados ISR en los entornos EW más agresivos.

El período de transición culmina con la iniciativa Army of Drones, del Ministerio de Transformación Digital ucraniano, lanzada el 1 de julio de 2022. Junto con los aparatos, meses después se han formado miles de operadores y pilotos. La intención declarada es que, en el plazo más breve posible, los combatientes regulares cuenten con sUAS (civiles o militares) de distintas características y roles, al nivel orgánico más bajo posible. El 30 de diciembre de 2022, el ministro Fedorov (15) anunció que se habían entregado 928 sistemas de los 1.577 financiados o donados por voluntarios nacionales o extranjeros. Si se piensa, son números ajenos a los que manejan las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado de los países europeos.

Uno de los principios universales de la guerra es que, en ausencia de victoria o derrota, los combatientes se adaptan y aprenden del contrario. En este caso, como dijimos, la Federación Rusa comenzó equipándose con sUAS militares de una gama muy reducida de modelos (*Orlan-10, Zala,* etc.). El daño que les han provocado los drones comerciales letalizados ha sido de tal entidad que han acabado por adaptarse a los medios y modos del adversario.

Entre los hitos de este proceso, destacamos el encuentro Dronnitsa (16). Del 1 al 5 de septiembre de 2022 se reunieron más de 100 droneros, *makers*, estudiantes universitarios y personas que se estaban introduciendo a marchas forzadas en el mundo de los sUAS. El encuentro fue centralizado a nivel nacional y aparentemente sistemático, si bien no podemos atestiguar su impacto posterior en las operaciones. A corto plazo, tiene que ser inferior, debido tanto a la experiencia previa ucraniana como al hecho de que su descentralización —como el «modelo bazar» de Raymond (17)— maximizan la transmisión de conocimientos y el ritmo de evolución de los productos. Este modelo sigue siendo incompatible con la organización militar rusa.

Con todo, no lograr los mismos resultados no es lo mismo que no lograr resultados. Las distintas fuerzas rusas (ejército federal, paramilitares, ejércitos

---

(13) *Ibidem*: entrevistas al líder de Drone Labs, M. *https://youtu.be/3o3T6gHdbIs*

(14) *Ibidem* (2022d): entrevista al portavoz de ArmySOS Ucrania, Oleksii Savchenko, *https://youtu.be/3sEIolfgmTU*

(15) *https://t.me/zedigital/2753*

(16) GREENWOOD, F. (2022): «Dronnitsa, A Conference for Russian Battle Drone Pilots». *Little Flying Robots*, *https://faineg.substack.com/p/dronnitsa-a-conference-for-russian*

(17) RAYMOND, E. S. (1997): *The cathedral and the bazaar*, *http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/*

privados, milicianos) se están dotando a nivel particular de los sUAS que pueden conseguir, y ya han tenido impacto en las operaciones. Tanto es así que los combatientes ucranianos informan de que hay momentos en los que tienen que emplear hasta la mitad de las horas de vuelo de sUAS para vigilar las fuerzas propias y asegurar que son lo menos detectables posible por parte del ecosistema sUAS militar y civil de los adversarios.

Estamos muy lejos de poder decantar lecciones duraderas y claras de este conflicto. Partiendo de esa base, el escenario inédito de miles de ojos en el cielo, al servicio de unidades de nivel orgánico cada vez más bajo, provoca una cascada de cambios en el movimiento montado o desmontado, en el camuflaje de posiciones, en el apoyo FAC (control aéreo avanzado) a la artillería, etcétera.

Aquí las fuerzas ucranianas cuentan con una ventaja adicional y de momento disruptiva: *la integración de los datos de los sUAS en distintos sistemas de gestión del campo de batalla,* que tanto reduce el tiempo del ciclo de gestión de la información como enriquece la conciencia situacional de los cuarteles generales y su toma de decisiones. Por una parte, tenemos DELTA, un BMS completo creado por el grupo Aerorózvidka y que ha acabado adoptando el Ministerio de Defensa. Por otra parte, está Kropivá, un conjunto *tablets android + software* que ofrece recursos GIS (sistema de información geográfica) a los artilleros y comunicación con los operadores de sUAS que aportan funciones básicas de FAC a las baterías e incluso piezas individuales. No se conoce un equivalente ruso a estos sistemas.

Peligros de mañana y su defensa

Casandra y Pandora resumen desde el mito la situación de los drones comerciales letalizados de 2023 en adelante.

Por una parte, tenemos un *coro de Casandras*: desde que los actores no estatales empezaron a hacer un uso eficaz de los drones comerciales letalizados, una y otra vez profesionales de muy distinto perfil (18) (19) han extrapolado a escenarios occidentales lo que estaba ocurriendo, y han advertido de las consecuencias de algunos hitos evolutivos. Y mientras los actores hostiles tomaban nota, los decisores institucionales europeos no han priorizado el problema ni han reaccionado a eventos con la intensidad adecuada.

---

(18) PLEDGER, T. (2021): *The role of drones in future terrorist attacks*. Association of the United States Army. *https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf*

(19) RASSLER, D. (2016): «Remotely piloted innovation: Terrorism, drones and supportive technology». *US Military Academy-Combating Terrorism Center at West Point, https://apps.dtic.mil/sti/pdfs/AD1019773.pdf*

Por otro lado, es completamente imposible cerrar la *caja de Pandora*: el conocimiento de *comunidad de práctica*, la estandarización y el *hardware* y el *software* libres se han diseminado tanto que la única opción realista es la de *convivir con la amenaza y trabajar en mantener y mejorar las probabilidades de éxito en su mitigación*. Mitigación, sí: una vez que un atacante ha superado la curva de aprendizaje, sus ventajas y posibilidades son tan amplias que no permiten asumir probabilidades de éxito adecuadamente bajas.

Por más que la plataforma sea lo que ya es, *el peligro fundamental siempre será la persona*: el pequeño grupo y el individuo aislado. El dron comercial letalizado tiene un potencial inédito para lograr impactos terroristas sin precedentes y para elevar a cotas no conocidas la denegación plausible. En muchos casos evita la necesidad de (mal-)gastar el recurso más poderoso y valioso posible, que es la vida de un operador entrenado. En el futuro, un salafista operativo no tendrá que convertirse en *shahīd* para alcanzar el éxito en sus propósitos. En su lugar, y siguiendo su etimología, podrá ser *testigo* a distancia de los resultados de su acción.

Sea como fuere, la amenaza de los drones comerciales letalizados no ha parado de evolucionar en esta media década y, a la vez, apenas ha comenzado a materializarse. El abanico enorme de modelos y capacidades se traduce en un rango incluso más amplio de amenazas y, sobre todo, de amenazados. Del VIP a la multitud, de la instalación crítica al arsenal o la base en el exterior, de los símbolos de la soberanía nacional al patrimonio natural; ninguno tiene ni va a tener una probabilidad de mitigación de la amenaza aceptable a corto plazo.

Para mejorar esta probabilidad de mitigación, el punto de partida es *conocerla*. Tanto los proveedores de soluciones Counter-UAS (C-UAS) como sus usuarios tienen la obligación de *mantenerse al día* si no quieren que la probabilidad favorezca demasiado al atacante. Y es fácil que esto ocurra: la variedad de los componentes de los sUAS comerciales y su ritmo de evolución son realmente elevados, especialmente los de autoconstrucción. Esto ofrece buenas oportunidades a individuos suficientemente talentosos para competir por el prestigio en las comunidades y para cooperar de cara a superar retos suficientemente intrigantes. Para terceros hostiles, este *pool* de talento y recursos es sencillamente demasiado tentador.

La *kill chain de la defensa contra UAS* es como toda cadena: tan fuerte como su eslabón más débil. Y cada eslabón principal presenta un problema muy complejo y mutable que exige la conjunción de diferentes recursos para mantener probabilidades favorables para el defensor. El modelo convencional *Find, Fix, Track, Target, Engage, Assess* (F2T2EA) puede simplificarse a dos etapas respecto a los medios C-UAS: detección (FFT) y respuesta (TEA) (20).

---

(20) TAN, C., *et al*. (2021): «System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment». *Systems,* 9(4) p. 79, *https://doi.org/10.3390/systems9040079*

Tanto en detección como en respuesta, el *operador humano está perdiendo relevancia* muy deprisa y ya es un factor secundario: sus tiempos de reacción naturales son ya insuficientes. En *Drones y Seguridad Nacional. Un estudio multidimensional* (21) (eje de estudio número 5), encontramos una síntesis completa del estado del arte de los sistemas C-UAS. El informe detalla el *gap* entre amenaza potencial y capacidades de defensa, y anima a reducirlo apuntando a los requisitos de un sistema C-UAS nacional y a un conjunto de buenas prácticas que compensen la actual falta de madurez tecnológica de dichos sistemas.

La variedad de las capacidades de los drones comerciales letalizados provoca que tanto FFT como TEA tengan que ser *multicapa y en evolución permanente* para aspirar a mitigar la amenaza de forma satisfactoria. Cada recurso C-UAS que se integre como capa será imprescindible para *mejorar la probabilidad de éxito del defensor*. Al conjunto de la industria de seguridad y defensa mundial se le está haciendo realmente complejo generar soluciones que sigan el ritmo de evolución de los sUAS, y mantenerlo apunta de nuevo al carácter crítico de mantener actualizado el conocimiento de la amenaza.

Futuros

Se ha planteado el presente en singular porque arrancamos de una singularidad: la explosión de posibilidades y la visibilización no negociable de las capacidades de los drones comerciales letalizados en el conflicto de Ucrania (22).

Hasta febrero de 2022, sólo las Fuerzas Armadas de Israel y de Estados Unidos invirtieron de forma significativa en la defensa contra esta amenaza. Aun en esos casos, los impulsores de esas medidas han tenido y siguen teniendo que luchar contra el obstáculo que supone la percepción de estos sistemas como *hobbyist's toys*.

Estos precedentes animan a pensar en una *salida heterogénea de la situación de singularidad*. La visibilización innegable no va a conllevar las mismas prioridades, tempos o claridad en la decisión para todos los aliados e incluso para todas las organizaciones supranacionales comunes.

Recordemos: la ventaja seguirá durante un tiempo en manos del atacante. Las posibilidades van a continuar siendo demasiado amplias, la barrera de

---

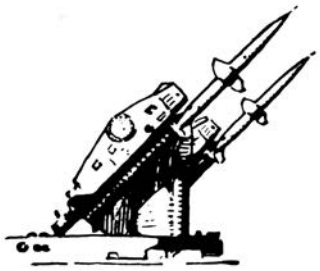
(21) *Drones y Seguridad Nacional. Un estudio multidimensional*, 2022. Consejo Nacional de Seguridad Aeroespacial, Gobierno de España, *https://www.dsn.gob.es/es/documento/drones-seguridad-nacional-un-estudio-multidimensional*

(22) KUNERTOVA, D. (2022): «The Ukraine Drone Effect on European Militaries». *Policy Perspectives*, 10. *https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-15_2022-EN.pdf*

entrada bajará antes que subirá y las relaciones riesgo/beneficios y coste/beneficios son demasiado elevadas. Sobre todo, la caja de Pandora se ha abierto definitivamente: hay demasiados ejemplos en redes sociales de lo mucho que han logrado muy pocos con tan poco.

Al mismo tiempo, la apuesta de todo el mundo desarrollado es por un crecimiento explosivo del uso civil y pacífico de los sUAS. El cielo del futuro (23) se acercará al imaginario de la ciencia ficción, aunque la gran mayoría de las aeronaves no serán tripuladas. La prohibición de los drones comerciales es ya tan probable como la del transporte de última milla.

El resultado: durante un período de transición, el mundo se dividirá entre los que se defiendan de la amenaza antes de que se materialice sobre ellos y los que se defiendan una vez sufran sus consecuencias. Tras ese período de transición, cada organización dedicada a la defensa estará obligada a mantener un proceso de evolución continua, porque nada invita a pensar que la evolución de los drones comerciales se vaya a frenar lo más mínimo.



(23) A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe». Comisión Europea, *https://transport.ec.europa.eu/system/files/2022-11/COM_2022_652_drone_strategy_2.0.pdf*