

Una acotación de la amenaza presente y futura de los drones comerciales letalizados

Juan Luis Chulilla Cano

Resumen

Comprender y acotar la amenaza presente y futura de los drones comerciales letalizados es, a la vez, un reto y una necesidad perentorios. El punto de partida más equilibrado es identificar algunos de los problemas que han impedido hasta 2023 identificar la amenaza, su prioridad y su potencial. Un juguete no puede ser un sistema de armas decisivo, por más que desde el campo llegaran advertencias sobre su uso.

El siguiente paso es abrir la caja negra y observar el interior: comprender, a cierto nivel de detalle técnico, qué se puede lograr con cada uno de los componentes con los que se han creado los drones comerciales y cómo estos sistemas, por separado y juntos, se traducen en un conjunto de capacidades militares disruptivas.

La suma de componentes y la apertura de la caja negra dejan ante una realidad muy diferente a la imaginada durante buena parte de este siglo: en lugar de *killer bots* autónomos o de enjambres autoorganizados que atacan de manera imparable, se encuentran sistemas sencillos, económicos y que alcanzan su verdadero y terrible valor gracias a lo que los operadores humanos logran hacer con ellos. Cuando los combatientes de ambos lados se sirven de sistemas parecidos, solo ellos pueden hacerlos evolucionar para mantener o reducir, según toque, cada ventaja competitiva.

Para maximizar esta carrera de la reina roja dronera¹, un nuevo ecosistema poblado por voluntarios, *war startups* e iniciativas gubernamentales, está reescribiendo el libro de reglas. Aprovechar lo que se pueda de sus ejemplos y monitorizar sus avances son pasos imprescindibles para pivotar el ecosistema de defensa C-UAS, hacer frente a la amenaza y, cuando sea posible, aprovechar la oportunidad.

Palabras clave

Drones comerciales, Drones FPV, Guerra de drones, Conflicto de Ucrania, Masa distribuida, Counter-UAS, Ecosistema de defensa.

¹ La carrera de la reina roja, un concepto derivado de *A través del espejo* de Lewis Carroll, se refiere a la necesidad de continuar avanzando solo para mantenerse en el mismo lugar.

An approach to the present and future threat of lethalized commercial drones

Abstract

Understanding and narrowing down the present and future threat posed by weaponized commercial drones is both a pressing challenge and a pressing need. The most balanced starting point is to identify some of the problems that have prevented identification of the threat, its priority and its potential until 2023. A toy cannot be a decisive weapon system, no matter how many warnings about its use come from the field.

The next step is to open the black box and look inside: to understand at some level of technical detail what can be achieved with each of the components from which commercial drones have been created and how these systems, separately and together, translate into a set of disruptive military capabilities.

The sum of the components and the opening of the black box leaves us with a very different reality from the one imagined for much of this century: instead of autonomous killer bots or self-organising swarms that attack unstoppably, we have systems that are simple, inexpensive and achieve their true and terrible value through what human operators manage to do with them. When combatants on both sides use similar systems, only they can evolve them to maintain or reduce each competitive advantage.

To maximise this red queen drone race, a new ecosystem populated by volunteers, war startups and government initiatives is rewriting the rule-book. Leveraging what we can from their examples and monitoring their progress are essential steps to pivot our C-UAS defence ecosystem, address the threat and, where possible, seize the opportunity.

Keywords

Commercial drones, FPV drones, Drone warfare, Ukraine conflict, Distributed mass, counter-UAS, Defense ecosystem.

1 El fantasma de Port Arthur

Tras más de 120 años, el lugar que ocupa la guerra ruso-japonesa de 1904-1905 en la historiografía militar se debe, en buena medida, a su papel como advertencia inadvertida sobre el papel que algunos avances tecnológicos iban a jugar en los siguientes conflictos de alta intensidad y, sobre todo, en los frentes principales de la Primera Guerra Mundial. La combinación de la ametralladora, el alambre de espino y la madurez de la pieza artillera de retrocarga y pólvora sin humo causó bajas sin precedentes y anunció las dificultades que introduciría para la guerra de movimientos.

Como es sabido, en las batallas de aquel conflicto hicieron acto de presencia observadores militares de las principales potencias del mundo. La gran mayoría de los informes llegaron a las mismas conclusiones sobre el efecto real de las últimas tecnologías desarrolladas. Sin embargo, el choque conceptual era tan profundo que ninguno de los contendientes de la Gran Guerra pudo incorporar a tiempo lo que deberían haber sido lecciones aprendidas.

En la fase de la guerra de Ucrania que arranca el 24 de febrero de 2022, el uso de los drones comerciales letalizados (de ahora en adelante, DCL) no ha sido una novedad. En distintos conflictos previos y, de hecho, en las etapas anteriores del conflicto, ya se habían empleado con éxito creciente, pero con poco impacto en la percepción de sus efectos más allá de algunos artículos precursores. De hecho, los éxitos del SOCOM norteamericano contra el DAESH y otros grupos salafistas y, en particular, la neutralización que lograron de la amenaza dron entre 2017 y 2018 tentó a no pocos a minusvalorar la amenaza e, incluso, a darla por mitigada de manera decisiva.

Una de las diferencias esenciales con la guerra ruso-japonesa estribaría en que, mientras que los altos mandos de comienzos del XX padecerían una ceguera doctrinal parcial y no fueran capaces de dar los últimos pasos conceptuales a los que llevaba la combinación de los nuevos medios industriales, en el caso actual los analistas y altos mandos tuvieron que luchar desde 2014 a 2022 con el aparente contrasentido de que un juguete como es el dron comercial (sobre todo, en comparación con los sistemas militares) pudiera tener un impacto significativo en las operaciones de alta intensidad.

En 2022-2024 apenas hay observadores militares aliados en primera línea, debido a las extraordinarias circunstancias que concurren en la guerra. En su lugar, las omnímodas redes sociales están trasladando imágenes reales del uso de los drones en primera persona (FPV - *First Person View*), abalanzándose sobre sus objetivos. Ahora mismo resulta muchísimo más difícil que en 1906 minusvalorar la amenaza, especialmente cuando se comprueba el impacto decisivo y paralizante que los pequeños drones

están generando en el invierno 2023-2024. Cabe confiar que no se va a repetir una situación comparable a la europea en 1914; sin embargo, hay que admitir que el ritmo de evolución de la amenaza es sustancialmente superior al ritmo de evolución y adquisición de los sistemas C-UAS. Está por ver si la necesaria y enérgica reacción a estas novedades se materializa, y será más probable cuanto mejor entendida sea la amenaza.

Lo que ya no está por ver es la similitud entre el efecto de la ametralladora y el alambre de espino con el efecto de la presencia masiva de los drones comerciales en el campo de batalla. La presencia de miles de ojos en el cielo, día y noche, con la sola y parcial excepción de la lluvia o la niebla densa, imposibilita desde hace meses que la concentración de vehículos previa al avance se ejecute sin ser detectada; perdida la sorpresa, a los efectores convencionales se les suma el dron volando a distancias de más de 10 km con una granada contramaterial o antiblindaje impactando con precisión en puntos desprotegidos. Como consecuencia, el movimiento ha quedado reducido a niveles anteriormente impensables y se lleva a cabo a costa de pérdidas difíciles de asumir. Los drones en su conjunto han frenado en seco la guerra de movimiento, como la suma de ametralladoras, artillería de retrocarga y alambre de espino hace cien años.

2 FPV vs comercial

La diferencia principal entre los drones civiles raya en lo filosófico. Por una parte, drones comerciales (como los de la empresa dominante DJI y de otras marcas como Autel, Parrot, Yuneek, Hubsan) se basan en el mismo principio: un producto cerrado, de muy difícil modificación y centrado en facilitar al máximo el manejo a los usuarios. Si desde el primer momento la interfaz y experiencia de usuario logró reducir decisivamente la barrera de entrada, en los últimos años los fabricantes líderes del mercado han añadido sucesivas mejoras orientadas a la evitación automática de obstáculos, la programación de rutas y un manejo cada vez más despreocupado, que permita al usuario centrarse en la grabación de tomas con fines personales o profesionales. Más una *appliance* que un dispositivo de vuelo, estos sistemas son productos diseñados para ser usados, no para ser modificados o mucho menos creados. Su enlace radio es sobradamente conocido por las FCSE occidentales, de manera que tal y como vienen de serie² son detectables en segundos por los sistemas C-UAS en uso.

Por otra parte, hay drones FPV. Son lo contrario a los drones comerciales en dimensiones muy diferentes. Hasta hace meses han sido por

² Tal y como vienen de serie. Si se modifica o sustituye su sistema operativo, su *firmware*, se pueden saltar las protecciones definidas de fábrica: límite de altura, límite de velocidad, zonas no-go y, sobre todo, anonimizarlos: evitar su detección por medios policiales.

completo minoritarios porque su curva de acceso era opuesta: elevadísima y con show stoppers³ de compleja solución. La mayoría de los drones FPV se han adquirido por piezas, de manera que el dronero y maker⁴ escoge los componentes que mejor encajan con el problema que quiere solucionar, con sus preferencias, etc. Una vez se adquieren los componentes físicos, electrónicos y de soporte el dronero-maker procede a montarlos en una cadena de pasos que lleva su tiempo y que demanda un importante set de conocimientos. Al acabar de montarlos, se instala y configura el firmware open source de la elección del dronero (betaflight, INAV, ardupilot, etc.). Después probar y finalmente volar, lo que a su vez exige un conjunto de destrezas completamente alejadas de las necesarias para usar un dron comercial - para que el dron pueda seguir trayectorias imposibles y recorrer al límite un circuito de carreras, o filmar instalaciones como nunca antes, su manejo está en las antípodas del mencionado uso despreocupado. El eterno retorno dronero de FPV sigue estos pasos: diseñar, montar, configurar, probar, volar, estrellar, empezar de nuevo.

No hay simetría: el usuario de drones comerciales no puede volar un FPV sin dotarse del conjunto de conocimientos y habilidades. El dronero FPV puede volar un DJI sin problemas.

Finalmente, hay que entender que el aeromodelismo clásico se vuela en tercera persona y tan lejos como el operador pueda distinguir con claridad la actitud de su aparato. Las cámaras FPV rompen esa barrera y colocan el límite teórico (que no el legal) en la distancia en la que se pueden seguir recibiendo imágenes del dron. Además, el set de habilidades y la experiencia es completamente distinta: el operador ve lo mismo que el dron y puede maniobrar de forma imposible para un vuelo en tercera persona. Muchos de los droneros FPV no iniciaron su camino en el aeromodelismo, sino que entraron desde la electrónica y el software: al fin y al cabo, un dron es un ladrillo lleno de electrónica, cables, cámaras y radios, que vuela.

3 One-way attack y ojo en el cielo

En la guerra, como desgraciadamente se está comprobando a diario, ambos tipos de drones se complementan: el dron comercial anonimizado (nota 1 a pie de página) se mantiene alejado de la línea de contacto y se aprovecha sus estupendas cámaras estabilizadas en tres ejes para obtener inteligencia a un nivel orgánico inéditamente bajo.

³ Obstáculo crítico que detiene o retrasa significativamente la adopción generalizada de una tecnología.

⁴ Mientras que «dronero» se refiere a una persona muy vinculada con drones de fabricación propia, que las mayoría de las veces los vuela y fabrica, «maker» es aquella persona que principalmente fabrica y modifica drones civiles a título particular.

En los cielos de Ucrania se asume que drones DJI Mavic y equivalentes son prácticamente desechables y se van a perder por efecto de la guerra electrónica. Sin embargo, las pocas horas que logren estar en el cielo son un recurso de inteligencia completamente inédito, que ha cambiado para siempre la historia de la guerra hasta el punto de ser uno de los componentes más importantes de las nuevas fuentes de inteligencia junto a los satélites comerciales para lograr el campo de batalla transparente (Taylor, 2024).

No se trata de una eliminación completa de la niebla de la guerra, tanto por motivos ambientales (niebla densa y lluvia intensa) como humanos (camuflaje aumentado y envenenamiento de computer vision); sin embargo, el hecho de que unidades de entidad sección o piezas de artillería individuales posean medios de reconocimiento aéreo orgánico y en tiempo real no tiene precedentes, como tampoco lo tiene que la información que generan esos medios alimenten distintos sistemas de gestión del campo de batalla.

La pura acumulación de cámaras volando día y noche dificulta no solo la concentración previa al movimiento, sino que reduce los fuegos de contrabatería a plazos inéditos de bastante menos de un minuto, reduce la movilidad cerca de la línea de contacto a muy pequeños grupos de infantes desmontados, y como se expresa en el manual de protección de infantería contra drones de las Fuerzas de Defensa Territorial de Ucrania: «La basura te puede matar. Si tiras una bolsa, una botella, un envoltorio, un papel al suelo, te has traicionado a ti mismo. Si no la limpias, el enemigo lo detectará. Recógela o entiérrala»⁵.

Hasta hace algunos meses, los drones comerciales también se empleaban para lanzar granadas y otras cargas letales volando en estacionario. Para ello se desarrolló una pequeña industria que fabricaba lanzadores activados mediante una célula fotoeléctrica activada por la linterna cenital del dron y un servomotor. Sin embargo, es una práctica que ha perdido mucho predicamento debido a lo conocido que es el radioenlace de DJI (Ocusync). Como quiera que en los drones DJI Ocusync se emplea tanto para control como para vídeo, resulta especialmente vulnerable a los sistemas de inhibición; además, su papel actual como vector de obtención de inteligencia es demasiado valioso como para arriesgarlos aún más en misiones tras las líneas enemigas. Es sencillo constatar cómo los ataques con lanzamiento de granada en estacionario y con interfaz de DJI han disminuido sustancialmente en el último semestre, a tenor de lo que se publica en redes sociales.

Los primeros drones de ataque creados por los droneros ucranianos se retrotraen a 2016. En otras piezas (en un artículo de la Revista General de Marina (Chulilla Cano, 2023) y en La guerra de Ucrania III (Murillo, López y

⁵ HOW TO PROTECT YOURSELF FROM THE ENEMY DRONES. TIPS FOR INFANTRY. Fuerzas de Defensa Territorial de Ucrania.

Piella, 2024) se cubre cómo grupos pioneros como Aerorozvidka desarrollaron los primeros multicópteros dedicados a observación y ataque nocturnos como el R-18. Estos drones pesados escapan del ámbito principal de este artículo, al tratarse de drones industriales que emplean componentes diferentes y presentan un coste y huella logística más elevados. Además, por más que jugaran un papel importante en los primeros compases de esta fase de la guerra de Ucrania (de febrero del 22 a la primavera del 23), su coste y complejidad impidieron que se consiguiera un factor crítico: la masa.

El problema no es solo que por cada dron pesado se pueden llegar a montar una decena de drones FPV o más, sino que las habilidades necesarias para hacerlo son aún más especializadas. Los drones FPV nacieron y evolucionaron por y para los aficionados y las empresas chinas que les sirven: una sola persona, en su dormitorio, con un soldador, un par de destornilladores y un PC puede montar un dron FPV.

El ecosistema FPV carece de precedentes militares. Grupos independientes aplicaron sus métodos de iteración (construcción, prueba, vuelo, repetir) al caso del dron FPV letalizado. En ciclos realmente cortos resolvieron los principales escollos que les separaban para poner en producción un dron que transportara de manera fiable una granada PG-7V contracarro o una mina direccional MON-50 a algunos kilómetros. Aprovecharon los desarrollos civiles para vuelos Long Range (pasar a baterías de ión de litio y mejorar la transmisión y recepción de los dos enlaces de radio), desarrollaron modificaciones de las cargas letales para poder ser empleadas sin sus medios originales y, sobre todo, mejoraron el *fieldcraft*⁶ partiendo de la metodología del tirador de precisión heredada de la URSS y adaptándola al enorme salto que supone no necesitar línea de visión con el blanco.

Un dron FPV de ataque es un efector sin precedentes. Puede torcer una esquina, quedarse en estacionario, dar media vuelta y reintentar la aproximación hasta que logra acertar a su blanco. Puede entrar por ventanas, troneras y cualquier rendija por la que quepa, y hacerlo a una velocidad tan lenta que resulta manejable para el piloto. La lenta velocidad de los drones FPV, comparada con la de un misil CC, ha supuesto otra ventaja sorprendente más: es mucho más manejable y permite esquivar obstáculos o cambiar la trayectoria mientras haya carga en la batería. Por si fuera poco, nunca antes se dispuso de esta suma de capacidades a un coste también sin precedentes: menos de 2000 € para un dron básico, probado y capaz de portar una carga útil de más de 2 kg.

⁶ El conjunto de habilidades del tirador de precisión relativos al camuflaje, observación y movimiento en entornos hostiles para tomar posición, identificar y neutralizar objetivos mientras se evita ser detectado.

Y con semejante ausencia de precedentes, no resulta sencillo acotar sus consecuencias. Solo hay una consecuencia evidente e indiscutible: los drones comerciales letalizados son la gran caja de Pandora de esta guerra. Han venido para quedarse, y ya han transformado las operaciones militares en un enorme abanico de aspectos. Además, la experiencia se está replicando de manera directa: el tsunami de innovación dronero ha llegado ya a Sudán, a Siria (esta vez en manos de las fuerzas del régimen de el-'Assad (Suleiman y Hezaber, 2024) y a cada vez más lugares de conflicto presente o potencial. A no mucho tardar, los DCL dejarán de ser opcionales, mientras que las Fuerzas Armadas de cada nación tendrán que priorizar más y más la integración y evolución de sistemas de sistemas C-UAS⁷. Aquellas naciones que apuesten con decisión por su ecosistema de fabricantes y proveedores de servicios C-UAS y por los campeones nacionales a cargo de la integración del conjunto de sistemas no solo protegerán antes y mejor sus recursos vitales, sino que apoyarán el crecimiento de este sector vía exportación.

4 El juguete y el teléfono volador

Se ha mencionado antes el freno conceptual que supone el juguete para valorar la amenaza que suponen los drones comerciales letalizados. Es un reto también sin precedentes: ¿Cómo han podido transformarse los protagonistas de las carreras de drones de la década pasada y los juguetes de navidad en un vector y efector con impacto significativo en las operaciones militares? No se habla del tamaño, o no solo: hay pocos drones comerciales tan pequeños como el Black Hornet de Teledyne y, desde luego, ninguno con esos 33 g de peso que se mantenga tantos minutos emitiendo vídeo a muchos cientos de metros.

De lo que se habla, fundamentalmente, es de aparatos voladores contruidos por aficionados en unos casos, y siempre operados por aficionados o, en casos contados, por profesionales en dominios por completo alejados de la milicia. Se trata de volar con drones FPV en pequeños circuitos de velocidad, de hacer acrobacias sobre ruinas o, bordeando la normativa aeronáutica, de volar más allá del alcance visual poniendo al límite habilidades y enlaces de radio. Todo, por algunos cientos o muy pocos miles de euros. Por el precio de un Black Hornet se pueden llegar a adquirir cerca de cien drones comerciales de distintas características. Otro precio que se paga en algunos casos son las horas de aprendizaje: mientras que un Black Hornet ofrece a su operador elevados automatismos, en el caso del dron FPV la curva de aprendizaje sigue siendo elevada y a todos los niveles: la mayoría de los operadores también son makers de sus propios drones y,

⁷ La inspiración inicial para esta formulación la proporcionó una conversación con Manfredo Monforte Moreno, general de división retirado.

en todos los casos, tienen que dedicar cientos de horas al simulador para adquirir las competencias necesarias para hacer lo que quieran con su dron.

La figura del maker merece reflexión aparte. Partir de unas decenas de componentes hardware y un software por configurar para llegar a un dron FPV en condiciones de vuelo es un camino largo y complejo que solo se puede construir en comunidad.

Sin embargo, no se habría dado ni el primer paso si la industria civil no hubiera generado los componentes necesarios. La explosión del smartphone no solo ofreció componentes imposibles de prever, como unidades de medición inercial que registran con precisión inclinación en tres ejes, aceleración y presión atmosférica, sino a un precio tan imposible como menos de 15 €. Hace no demasiados años, sus equivalentes subían de precio y, sobre todo, masa en varios órdenes de magnitud. Los drones FPV de cuatro motores, los famosos quads o cuadricópteros, pueden mantenerse en vuelo gracias a que la CPU recibe a amiles de veces por segundo datos precisos de inclinación y aceleración y, con ellos y las lógicas de su programación, puede traducir los comandos del operador en cambios de actitud y aceleración controlables. Si el operador tuviera que mantener la velocidad de cada uno de los cuatro motores por separado, sería imposible un vuelo controlado.

No es el único ejemplo del imperativo de la electrónica de consumo sobre los drones comerciales. Se puede hablar de protocolos de radio definida por software, de gran alcance y de bajo consumo, que, emitiendo a menos de 2 W, alcanzan muchos kilómetros en condiciones óptimas, ofrecen salto de

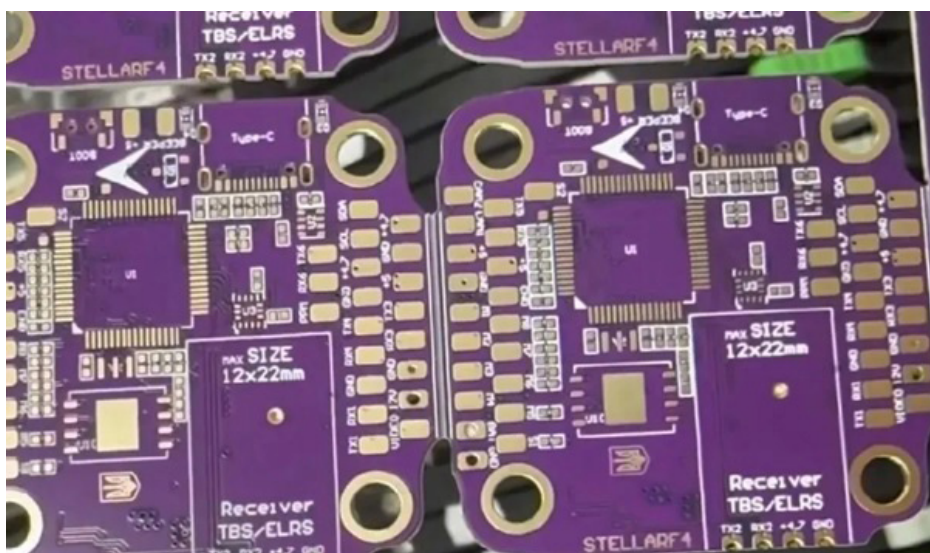


Figura 1. Placas controladoras de vuelo del grupo ucraniano Wild Hornets.
© Forbes

frecuencia encriptado dentro de las frecuencias legales⁸, de *firmware* (sistema operativo embebido) libre, gratuito y de enorme capacidad y adaptabilidad, o incluso de diseños de *hardware* libres y disponibles para ser implementados con recursos realmente reducidos. De hecho, a principios de 2024 se ha cerrado el círculo y pequeños grupos ucranianos como Dyki Shershni (Wild Hornets) han empezado a fabricar (*In Ukraine flight controllers for drones have been developed*, 2024) placas de controladoras de vuelo integrando sus componentes principales gracias a que los diseños y esquemas estaban disponibles en su totalidad.

En este sentido, el miedo a un *shadow ban* (prohibición encubierta y no declarada) de componentes chinos a Ucrania es cada vez mayor, y con ello crece la presión —y la oportunidad— para que distintos fabricantes ucranianos y occidentales disminuyan la dependencia de los componentes chinos, especialmente electrónicos.

5 Software libre, componentes abiertos, comunidad

Este conocimiento libre y acumulado en comunidades de práctica online nacionales e internacionales, es esencial para que el dron FPV haya evolucionado primero como dispositivo civil y ahora como vector y efector militar. En las manos y mentes más talentosas posibles, el conjunto de componentes necesarios para construir un dron se puede escoger, modificar e incluso fabricar para optimizar la respuesta a una necesidad dada. Por ejemplo, desde antes de febrero del 2022 los voluntarios ucranianos habían seguido la tendencia dronera internacional a sustituir las baterías de polímero de litio por otras de ion de litio... construidas por ellos mismos. Las baterías, basadas en baratas celdas estándar de ion de litio (18650, 21700, etc.), ofrecen una mayor densidad de carga que resulta crítica para mantener el aparato en vuelo durante más minutos. Las conocidas y también comunitarias impresoras 3D permiten modificar los marcos o frames de los drones para optimizar su rendimiento (por ejemplo, asegurando posición de antena GNSS para evitar la interferencia con otros componentes eléctricos), o aportarles nuevas funcionalidades, como sistemas de suelta de carga basados en servomotores y piezas creadas *ad hoc*.

Mención especial merece el uso de las impresoras 3D para modificar las cargas útiles letales. De las granadas de 30 y 40 mm modificadas crudamente para permitir su detonación sin haber sido disparadas y con alas impresas para mejorar su comportamiento lanzadas desde un dron, se ha pasado a generar distintas municiones de fragmentación optimizadas

⁸ O desde hace unos meses fuera de la legislación internacional, que han logrado tanto ucranianos como rusos al modificar los emisores y receptores ELRS para emitir desde 720 MHz hasta casi 1000 MHz partiendo del set inicial en 868 / 915 MHz.

para las dimensiones de un dron. No hay que explicar el efecto que una Claymore o una MON-50 pueden crear si detonan en ángulo en lugar de detonar a ras de suelo.



Figura 2. Granadas VOG modificadas con aletas impresas en 3D para su uso con drones. © Getty Images

Los drones FPV nacieron y pudieron madurar gracias a las comunidades de entusiastas. Ingenieros, hackers y personas de las profesiones más variadas se unieron a foros, primero, y grupos en RRSS, después, para compartir conocimientos y aprender juntos. Comparados con las comunidades de Linux, hay que señalar que la cordialidad y la cooperación son superiores y, por motivos muy prácticos, solo se puede mandar a Read The Fucking Manual cuando hay un manual que leer. Una vez más, nadie podía imaginar que esas comunidades se reconvertirían en una forma completamente



Figura 3. Makers Ucranianos montando un dron para la guerra. © Aleksey Filippov/AFP

nueva de innovar en la guerra: el ecosistema de grupos voluntarios y war startups ucranianos, imitado en cierta medida por sus adversarios rusos.

No se puede acabar la revisión del software sin mencionar los simuladores. Se trata de piezas críticas para el aprendizaje de los futuros pilotos. Por menos de 50 € (o completamente gratis en algunos casos de software libre), y empleando un PC con windows y una tarjeta gráfica que no sea nada del otro mundo, un usuario puede conectar la emisora que luego empleará para operar su dron y aprender a pilotar. Pese a esta ayuda decisiva de la controladora y sus sensores, la operación de un dron FPV no es sencilla... porque sus creadores originales no desarrollaron el software para que fuera cómodo, sino para extremar la agilidad y velocidad de respuesta.

Los simuladores en PC ofrecen al operador un entorno de vuelo crecientemente realista en el que adquirir y mejorar habilidades de vuelo sin importar las miles de veces que acaban estampando su dron simulado contra el suelo o un obstáculo. Desde el primer momento, los simuladores de vuelo han resultado ser un recurso indispensable: es básicamente imposible volar un FPV a la primera, y a poco brusco que sea el choque se van a partir hélices, o patas, o dañar los componentes electrónicos. De hecho, el aprendizaje en simulador se ha integrado en los currícula de pilotos ucranianos y rusos como elemento esencial en el que formar primero a decenas, luego a cientos y ahora mismo a decenas de miles de pilotos que saquen partido a la montaña de drones FPV que se está poniendo en servicio en 2024.

El simulador ha ganado valor con la guerra, porque permite al aspirante a dronero de combate entrenar miles de veces hasta perfeccionar su arte. De hecho, en fecha muy reciente se ha liberado en Steam un juego llamado «FPV Kamikaze» que ha dado el salto a la simulación de operación de combate de drones en entornos comparables a los de la guerra de Ucrania, empleando los drones de manera comparable a cómo se emplean en el conflicto. Hay que señalar que la física del dron no es tan precisa como los productos estrella (Lift Off, Velocidrone) y, sobre todo, el origen del software desaconseja su instalación en un ordenador de uso cotidiano.

6 La radio voladora

Las radios analógicas permitieron que los aeromodelistas tomaran el control de sus creaciones sin recurrir a cables. De hecho, los primeros drones FPV heredaron ese recurso crítico que permitía emitir comandos desde la emisora hasta el receptor de radio (RX) montado en el dron. Al igual que ha ocurrido en el caso de los smartphones y del resto del monstruoso ecosistema digital inalámbrico, la introducción de la radio definida por software ha permitido un salto disruptivo. Un RX digital pesa 0,7 g (10 g sumando antena y conector) y garantiza la recepción de la señal procedente de la emisora desde no

pocos kilómetros para una potencia de no demasiados miliwatios. Además, el enlace le permite devolver datos de telemetría a unos hercios respetables.

Los protocolos más populares en 2024 (Crossfire y ELRS) no difieren ni en frecuencias ni en tecnologías empleadas de manera decisiva. Ambos ofrecen una bajísima latencia y permiten un salto de frecuencia dentro de la banda empleada al emplear tecnologías FHSS (*Frequency Hopping Spread Spectrum*). La diferencia más importante es que Crossfire es un protocolo privativo y cerrado, mientras que ELRS es abierto. Esto se traduce en que un RX crossfire cuesta menos de 50 €, mientras que uno ELRS cuesta menos de 20.

Como se ha comentado líneas arriba, el hecho de que la licencia de ELRS sea *open source* ha permitido emplear otros protocolos igualmente libres (concretamente, LoRa) y adaptarlos del propósito original de enlazar nodos con poco ancho de banda pero muy largo alcance en una red Mesh a una red punto a punto (entre el TX y el RX) de bajísima latencia. Tanto el enlazado (*bind*) entre emisora y receptor como los pasos de frecuencia se emplean encriptados para evitar que un tercero tome control del dron mientras está en vuelo. El origen del salto de frecuencia se debe a las carreras: como quiera que los pilotos van a emplear un número reducido de bandas de frecuencia (868/915 ó 2.4, fundamentalmente) era crítico que no se interfirieran para volar con muy pocos metros de separación. Claro está, esta característica le pone las cosas más difíciles al defensor que emplee sistemas de inhibición, al tener que cubrir bandas más amplias.

Estos protocolos y sus frecuencias se diseñaron y escogieron para lograr una buena penetración. Los pioneros de la dronería FPV enseguida le cogieron el gusto a volar en el interior de edificios abandonados, esquivando obstáculos y entrando y saliendo por sus aperturas. Una vez más, estas características inocuas han sido reaprovechadas para superar los obstáculos entre el emisor y el receptor y, por ejemplo, lograr penetrar en el interior de instalaciones con fuerte componente metálico hasta alcanzar sus objetivos.

El radioenlace que terminó por permitir el vuelo en primera persona fue el que transmitía una señal de vídeo con latencia mínima y a distancia.

7 La cámara voladora

Los drones FPV (*First Person View*) transformaron tanto el aeromodelismo como el uso profesional e industrial de los drones de categoría I y peso inferior a 25 kg. o, según normativa europea, todos los drones de categorías C0 a C3. Una vez que se solucionó el problema de la miniaturización de los emisores de vídeo por radiofrecuencia (VTX) haciéndolos ligeros, de poco volumen y baratos, nació una afición y luego una profesión netamente distinta. De hecho, es el secreto del éxito inicial de la dominante DJI:

levantar un dron con una cámara (el primer Phantom) que pudiera enviar un feed de vídeo a su receptor a cierta distancia y en tiempo real.

Desde sus inicios, las cámaras montadas en dron han dado lugar a un rango creciente de usos profesionales civiles. La base es el control del dron: gracias a la cámara, el operador puede controlar su dron fuera del alcance visual y sin necesidad de preprogramar su trayectoria. Si la cámara ofrece resolución suficiente, permite emplear al dron para todo tipo de tareas de inspección y observación. Si no es el caso (por ejemplo, casi todas las cámaras de señal analógica), hasta hace no mucho se montaba una cámara de acción solidaria a la cámara FPV para grabar secuencias de alta calidad. Ese problema se ha solucionado en fecha reciente gracias a los sistemas VTX digitales, que ofrecen tomas sin pérdidas y de alta calidad para todo tipo de grabaciones publicitarias.

Anteriormente a las cámaras FPV, los aparatos de aeromodelismo (que no se denominaban drones) tenían que controlarse en alcance visual, lo que limitaba mucho su uso para aparatos de tamaño reducido. Sumando estos primeros y primitivos emisores de vídeo a drones con una relación empuje/peso excelente, nacieron las principales modalidades de vuelo FPV: enloquecidas carreras de obstáculos, vuelos freestyle acrobáticos en todo tipo de entornos, y vuelos long range mientras fueron legales o al menos no despertaron la alarma de las autoridades competentes. El factor de diversión y competición entre aficionados es de tal magnitud que, de hecho, para estos talentosos jóvenes, y no tan jóvenes, era realmente difícil de imaginar el uso hostil y malintencionado de sus preciados drones.

Los aficionados, y ahora algunos profesionales, han pasado a pilotar sus drones con gafas FPV en lugar de con monitor externo. En vuelos con muy poco margen para el error, las gafas permiten concentrar por completo al piloto en el feed de vídeo que recibe en tiempo real mientras maneja una emisora cuyos mandos conoce por memoria muscular. La sensación de estar en el dron llega a ser completa y resulta crucial para arrancar al rival unas décimas de segundo o para ejecutar una maniobra imposible, entrando y saliendo por una chimenea de una fábrica abandonada.

El vídeo puede derivarse a otros dispositivos. De hecho, muchos binomios en la guerra de Ucrania operan así: mientras el piloto se concentra en su misión, su binomio obtiene inteligencia del feed de vídeo y ayuda al piloto a la navegación y a evitar amenazas.

Nadie pudo prever, hasta que ha sido evidente para todos, el valor del feed de vídeo generado durante el vuelo. Es tanto un recurso de battle damage assessment que además se combina con las imágenes a distancia de los drones comerciales como un recurso adicional de inteligencia general. Conviene detenerse en este punto como un todo.

En el cambio de siglo, la introducción generalizada de drones tácticos, MALE y de categorías intermedias produjo un interesante cuello de botella: la IMINT de los feed de vídeo de los drones. En algunos momentos de la guerra global contra el terror, una proporción muy significativa de los feeds de los drones no llegaba a ser aprovechado. De la misma manera, el valor de los feeds de los drones tácticos mayoritariamente quedaba concentrado en la unidad para la que eran recurso orgánico. Con este panorama, parece claro que el cuello de botella aumentaría de forma proporcional al número de ojos en el cielo de forma simultánea.

Si hubiera ocurrido así, los drones comerciales no habrían ganado la preponderancia que han logrado. Sucede, para empezar, que el aumento de drones ha llevado aparejado un aumento del ancho de banda humano. El mencionado binomio, y otros miembros de la unidad, aportan capacidad de IMINT distribuida, interpretando el feed, detectando objetos de interés adicionales y generando battle damage assessment. La aportación decisiva de los drones al campo de batalla transparente se completa cuando toda esta inteligencia se canaliza y suma empleando los distintos sistemas de gestión del campo de batalla (BMS).

En la medida en la que lo permiten las comunicaciones de una zona (fundamentalmente starlink, pero no solo), el feed de vídeo o al menos fragmentos significativos ascienden a escalones superiores; sin embargo, lo importante es que la información operacionalizada consume un ancho de banda despreciable y puede ser mantenido empleando distintos sistemas de comunicación (incluso civiles en circunstancias puntuales). Esta capacidad aumentará más aún conforme se incorpore más y más el tratamiento multimodal de la información en bruto y los modelos de IA detecten objetos de interés; con todo, conviene poner en valor lo conseguido aquí y ahora combinando miles de ojos en el cielo, miles de mentes humanas, varios sistemas de gestión del campo de batalla y sistemas de comunicación redundantes. Sobre todo porque, saliéndonos del actual conflicto, se trata de una capacidad al alcance de algunos actores no estatales.

El vídeo producido por los drones comerciales se ha revelado como un recurso de propaganda sin precedentes. Los vídeos de los ataques con drones FPV y comerciales comenzaron a llegar en fecha temprana a redes sociales y constituyeron un éxito instantáneo. Estas secuencias siempre llamativas las emplean los grupos droneros independientes para algo tan mundano como conseguir visitas para sus canales. La batalla por la economía de la atención era y sigue siendo completamente crítica, los grupos droneros necesitan la atención de su público para conseguir donaciones que les permitan comprar todo tipo de componentes y equipos.

La publicación recurrente de los vídeos de ataque de los drones ha tenido un impacto muy significativo en el público general y hasta

especializado. Los datos OSINT han pasado a depender cada vez más de los vídeos de los grupos droneros, y, por lo tanto, es razonable asumir un sesgo FPV importante en la causa de las bajas rusas de vehículos constatadas y, en menor grado, en las ucranianas.

8 El dron NLOS

Se comenzó esta fase de la guerra con una experiencia limitada con drones FPV letalizados. Eso ya se había traducido en alcances de hasta 4 km, empleando antenas direccionales de alta ganancia montadas sobre mástil portátil y los mejores componentes VTX y RX disponibles. Esto permitió, a su vez, separar la antena del operador. Esto ha ganado una importancia capital para el fieldwork de los operadores y es un aspecto muy importante en la formación de los droneros de guerra en las academias: los operadores, como los tiradores de precisión, aprenden a moverse y ocultarse. Al contrario que los tiradores, los droneros de combate no necesitan línea de visión directa a blanco alguno. Esto les permite emplear ruinas, búnkeres a cierta profundidad o cualquier otro escondite discreto desde el que sacar sus cables.

Este principio se ha extendido en fecha reciente al uso de drones relé o repeaters: un dron se sitúa en estacionario a más de 100 m de altura, recibe la señal de vídeo del dron FPV y la transmite al dronero en tierra. La señal de control sigue el camino inverso, de la antena del dronero al dron relé y



Figura 4. Sistema de relé ucraniano instalado sobre DJI mavic. https://twitter.com/front_ukrainian/status/1745906821871612023

de este al FPV. El resultado es que el máximo tiempo posible se mantiene línea de visión sin obstáculos entre el FPV y el relé, y con ello ambas señales se degradan lo menos posible.

Además, este sistema se ha empleado junto con modificaciones por hardware y software para alterar las bandas de frecuencia de las parejas de emisor y receptor. Hackers RF ucranianos y rusos han modificado el firmware de los sistemas ELRS para emplear bandas diferentes a la de 868 y 915 MHz, llegando a 1015 MHz y bajando hasta 740 MHz, y, en algunos casos, han modificado los emisores con amplificadores de señal y/o empleando placas de relé que permiten un cambio de la banda de frecuencia empleada. El resultado de todas estas innovaciones combinadas es que se ha pasado de 4-6 km, en el mejor de los casos, a récords de 22 km y alcances relativamente habituales de 10-12 km. Hasta fecha reciente, la limitación para la autonomía del dron FPV de ataque había sido el alcance de sus radios. Con un relé se puede aprovechar las baterías de ion de litio para alcanzar esos 22 km en algo menos de quince minutos, y ofreciendo inteligencia durante todo el trayecto.

No se debe olvidar que el dron relé va a operar en zona amiga, razonablemente lejos de la línea de contacto y en estacionario. Será relativamente raro que se pierda. El coste de cada misión será el del dron FPV creado y testado con componentes de la máxima calidad a la que se tenga acceso. Ahora imagine el lector lo que implica llevar a 22 km un dron contra carro, que va a poder atacar a un MBT por detrás y desde arriba. Por el coste de un Spike NLOS se pueden adquirir y poner en servicio aproximadamente cien de estos drones. Y por el coste de un T-90M, se pueden adquirir más de mil de estos drones. Las distancias que se están logrando permiten ya el fuego de contra-batería contra morteros y, en casos excepcionales, contra piezas de artillería. Sin embargo, la amenaza principal de estos drones FPV de alcance extendido se cierne sobre los medios logísticos. Efectivamente, los últimos kilómetros hasta las posiciones defensivas están ya completamente dentro del alcance de estos drones, más baratos que cualquier blindado, camión, 4 x 4 o incluso UGV (Unmanned Ground Vehicle). En la reciente batalla de Avdiivka (culminada en febrero de 2024) se comprobó cómo los drones FPV rusos resultaron críticos para estrangular el suministro a los defensores y provocar que la retirada no se llevara a cabo en las mejores condiciones posibles.

9 La IA voladora

La IA es, en parte, producto de una narrativa cultural industrial, el paso de Pygmalion al Gólem, la creación independiente que se vuelve contra su creador y contra la sociedad, y que acaba en HAL-9000 y Terminator. Esta visión ha contaminado el análisis del estado del arte de la IA, aplicada a vectores y efectores del campo de batalla. Queda fuera de este análisis su aplicación crítica a los sistemas de gestión del campo de batalla.

En el imaginario de Defensa, y, por supuesto, en el del gran público, los drones son uno de los sistemas que se conectan con más asiduidad al concepto inicial de IA. De hecho, las campañas políticas norteamericanas (tan bien financiadas y sostenidas en el tiempo como mal justificadas) han iterado en la última década y media en torno al *Killer bot*, *Slaughterbot* o al concepto de *Autonomous killing*⁹. Uno de los ejemplos de ficción que se pretende aviso sobre el futuro es, precisamente, *Slaughterbots*, un vídeo corto del Future of Life Institute¹⁰, una organización sin fines de lucro dedicada a prevenir las amenazas existenciales y, concretamente, la que presuntamente supone la IA avanzada. Probablemente hayan visto el vídeo en youtube y se habrán percatado de que no es un vídeo de youtuber, sino una producción profesional y con recursos significativos.

No cabe aquí extenderse sobre los sistemas de armas que, desde hace años, son necesariamente autónomos en su *kill chain*. Desde los Active Protection Systems de los blindados a los sistemas AEGIS, hay un rango de sistemas de defensa para los que los tiempos humanos no son compatibles con la misión encomendada. De la misma manera, el salto tecnológico final de la Guerra Fría propició la aparición de una amplia diversidad de efectores contra carro de guía terminal autónoma. Muy acertadamente, se estimaba que la forma de gripar el rodillo blindado PACVAR¹¹ residía en emplear en masa una combinación de efectores NLOS¹² que detectaran y atacaran por sí mismos a los blindados.

El dron convertido en *killer bot* es un animal completamente distinto. Los activistas los presentan como pequeños drones que no solo navegan por sí solos, sino sobre todo que deciden y ejecutan el empleo de la fuerza letal contra seres humanos. El problema principal que genera esta visión es que al militar al cargo de la decisión se le priva del mando y el control, de la decisión de qué y cuándo, pero no de la responsabilidad. Además de esta perspectiva tan poco halagüeña, el problema conceptual más grave es el de sustitución en vez de aumentación: la inteligencia artificial se plantea

⁹ *Killer bot* y *slaughterbot* son términos sinónimos creados mayoritariamente desde fuera del dominio de defensa y que apuntan a dispositivos no tripulados, mayoritariamente drones, que actúan con entera independencia de la decisión humana. *Autonomous killing* sería un uso de la fuerza letal con independencia de la decisión humana y con el énfasis puesto en el peligro para la humanidad en su conjunto.

¹⁰ Véase: www.futureoflife.org

¹¹ Recuérdese el escenario más temido y visibilizado de conflicto convencional en Europa durante los setenta y ochenta. La masa blindada del Pacto de Varsovia, cerca de un orden de magnitud superior a la disponible para OTAN, tendría capacidad para romper las sucesivas defensas y llegar a sus objetivos en muy pocos días a menos que se empleara una cantidad aún más masiva de efectores contra carro.

¹² *Non Line of Sight*. Efectores que no necesitan que, en todo momento, el operador observe de manera directa a su blanco, sino que poseen algún tipo de sensorización o guía que les permite guiarse una vez lanzados, sobre todo en la fase terminal.

como sustituta en lugar de como aumentadora de la humana, despreciando la flexibilidad, adaptabilidad y juicio humanos cuando el individuo dispone de tiempo para decidir.

Matar personas es propio de asesinos o de proyecto de genocidas, no de las operaciones militares. En las operaciones militares el uso de la fuerza letal es un medio al servicio de los objetivos planteados, sometido a las reglas de enfrentamiento y al criterio personal del mando al cargo; además, dichos medios van a ser por definición limitados, y una decisión no humana va a ser siempre inferior al juicio humano sobre cuándo y qué.

El problema de los *killer bots* es que se trata de artefactos de la imaginación. Trasladados al terreno de lo real, se hablaría de montar en un dron de pocos cientos de gramos dos unidades de procesamiento: una TPU o unidad de procesamiento de tensores, en la que ejecutar el o los modelos de machine learning, y una companion computer que le haga peticiones a la TPU y convierta sus resultados en órdenes para la controladora de vuelo del dron. Este montaje no solo sería más grande que un dron pequeño, sino que consumiría una potencia muy importante comparada con la que consume un motor trifásico de dron. El resultado de esto es que el film *slaughterbots* es y seguirá siendo fantasía malintencionada y en conflicto con lo que en el futuro a medio plazo va a poder miniaturizar la electrónica.

La visión del Golem fuera de control es muy eficaz para arrebatar la atención a lo inmediato y posible. La aplicación más avanzada, pero real, de los sistemas de IA es la navegación por seguimiento de terreno empleando una cámara y computer vision. En entornos de navegación vía GNSS imposible o denegada, el sistema puede reconocer los hitos del entorno que le permitan completar un circuito. En la actualidad es una capacidad restringida a los UAS más avanzados, sobre todo militares. Pero los avances en los componentes necesarios acercan una solución de coste contenido y licencia libre, aunque con limitaciones de peso y tamaño.

Por otra parte, existe la guía terminal autónoma. Como se ha comentado antes, el dron que cerrara la fase terminal de su vuelo con una *kill chain* completa no necesita inteligencia artificial para hacerlo... de forma probabilística. La detección de un blindado dentro de un área autorizada para hacerlo es un problema resuelto hace décadas (submuniciones como las Skeet o la BAT, por ejemplo), siempre que se acepte cierto margen de fallo (incluyendo empeñar un blanco ya destruido) y que no se busque un punto de impacto específico del carro.

En los años ochenta surgen sistemas CC más allá de la línea visual que ofrecen al tirador un feed de vídeo en tiempo real con el que mantenerse en el loop y decidir: dónde exactamente, y si hacerlo. En 2023 y 2024 se aplica el mismo principio de uso de un Spike NLOS, solo que rebajando más de

dos órdenes de magnitud su precio. El operador pilota el dron FPV gracias a su feed de vídeo y decide exactamente dónde y si hacerlo.

En este momento pivotal de la historia de la tecnología, el mencionado dilema entre sustitución y aumentación del hombre puede tentar a algunos a minusvalorar las capacidades de una mente humana entrenada, desde el juicio humano pasando por la flexibilidad y la improvisación. El dron *killer bot*, así, pasa por alto lo que una persona motivada y preparada puede llegar a hacer con un dron en las manos.

Es cierto que la inhibición de los enlaces radio, y especialmente el de control, supone un grave problema para el piloto humano de un dron FPV. Ahí es donde ya está entrando la guía terminal autónoma, pero no como IA avanzada sino como recurso más probado y sencillo: cuando el piloto quiere o tiene la oportunidad, y a distancia prudencial, coloca el punto de mira de su cámara donde quiere que impacte el dron. A continuación, pulsa uno de los controles de su emisora para transmitir al dron la orden de que se dirija en línea recta a ese objetivo. Para cumplir esa orden no hace falta una IA avanzada ni una TPU enorme: recursos plenamente maduros como el *optical flow* (comparable a las guías de munición por TV de los sesenta, pero miniaturizado) hacen perfectamente el trabajo. A fecha de febrero de 2024 no se ha alcanzado un grado de madurez suficiente que permita la generalización de esta capacidad, pero cada vez le queda menos.

10 Enjambre y masa

Más allá del aquí y el ahora, está una capacidad muchas veces anunciada y hasta ahora no concretada: los enjambres. Hay que destacar la asombrosa dificultad del problema: un enjambre propiamente dicho es un conjunto de drones que comparte información proveniente de sus sensores y coordina entre sí sus acciones individuales y en grupo «votando» sobre el curso de acción más apropiado según evolucionan las circunstancias para lograr el mayor éxito posible de una misión. Por ejemplo, si un enjambre pierde parte de sus integrantes durante el transcurso de una misión, los supervivientes conocerían este hecho y adaptarían sus perfiles de vuelo y misiones particulares para que la misión general se cumpliera lo mejor posible.

Dificultades: ancho de banda, comunicación segura (futuro: lumínica), capacidad de cálculo in situ y, sobre todo, complejidad software. No hay nada ni remotamente similar en la definición de agentes en los repositorios libres. Las compañías más avanzadas dan pasos hacia la implementación de sistemas de comunicación altamente resistentes (incluyendo la comunicación vía láser, así como redes mesh de baja latencia y gran ancho de banda), y sobre todo software que genere para todo el enjambre una

common operational picture y acerque la adaptabilidad colectiva a la puesta en servicio.

En cualquier caso, hay que insistir en que se lleva décadas debatiendo y avisando sobre una tecnología que no acaba de ser puesta en producción. Tanto espacio ocupó en las discusiones que hizo todavía más invisible al juguete, al dron construido a base de piezas estándar y software libre y, sobre todo, a las mentes que los conciben, los fabrican y los vuelan. Un efector aparentemente menos rupturista que el imaginado enjambre gestionado por agentes de inteligencia artificial, ha acabado resultando completamente disruptivo. En lugar de una masa de drones atacando simultáneamente y por sí mismos, lo que ha traído esta guerra es un goteo continuo de vuelos, de día y de noche, sobre amplios sectores de la línea de contacto que se transforma en un todo continuo de vuelos sobre cualquier blanco posible.

El verdadero peligro en 2024, el concepto central respecto a la letalización de los drones comerciales y FPV es la masa distribuida. Una realidad que, sin ser enjambre, se adapta en mil direcciones y a un ritmo más que preocupante. Como decía Koba el Terrible, alias Iosif Stalin, la cantidad tiene su propia calidad. No es sencillo definir un momento preciso o una cantidad en la que el uso de los drones cambia de fase. De hecho, en mayo de 2023 el británico RUSI publica *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine* (Watling y Reynolds, 2023). En este informe se señala cómo Ucrania estaba perdiendo 10 000 drones al mes. Dejando aparte lo redondo y, por lo tanto, grueso de la cifra, lo importante es que en aquellos días no se acababa de visualizar el cambio que estaba teniendo lugar: la gran mayoría de las pérdidas no eran tales, sino el resultado inevitable del uso de los OWA (One-Way Attack) drones, mal llamados entonces y aún ahora *Drones kamikaze*. Todavía no se había establecido en Ucrania una cadena de suministro que permitiera consumir ese número de drones, pero a no mucho tardar la cadena logística y de producción escaló a lo que acabaron siendo las cifras estables: cientos de miles al finalizar el año, millones en 2024 y sucesivos. Y otro tanto ocurría y ocurrió con los pilotos: de cientos se pasó a miles y luego a decenas de miles.

La masa, así, no es la imagen de una bandada de drones en un render publicitario, por más que hasta hoy una parte significativa de los sistemas C-UAS se ilustren actuando contra esas formaciones aún inexistentes. La masa es un producto del empleo de drones comerciales y FPV durante enormes períodos de tiempo. En un evento de alta intensidad sobre los cielos de Zaporizhzhia o Jersón podrán estar volando a la vez menos de diez drones¹³ en una distancia de pocos cientos de metros. Sin embargo,

¹³ La mayoría de las veces el límite lo marcarán el número de emisores de vídeo que puedan operar en las cercanías de forma simultánea.

en el transcurso de unas horas seguirán apareciendo más y más drones, individualmente o en pequeños grupos, conforme se detecten nuevos blancos. La masa no va a ser instantánea, sino acumulada y distribuida, y muy probablemente los efectos son peores de lo que cabría esperar de un imaginado enjambre de cientos de drones volando durante unos minutos sobre un área.

11 Chimple vs expenplex: economía del dron

Las cifras mencionadas son una de las disrupciones principales de los drones comerciales letalizados. El final de la Guerra Fría y la era de los dividendos de la paz marcaron una clara tendencia a los productos exclusivamente de defensa, barrocos (Kaldor, 1983) y expenplex: *expensive and complex*. Sistemas magníficos, en lo posible multirrol y avanzando decisivamente las capacidades respecto a la generación de sistemas anteriores, fueron la norma por tierra, mar y aire. El dron comercial es uno de los abanderados de la era de los sistemas chimple: *cheap and simple*. La concentración de roles y capacidades se desacopla hasta donde es posible, y la reducción de costes en varios órdenes de magnitud deriva del empleo de tecnologías civiles, que en el caso de las digitales no solo son suficientemente baratas, sino que superan en capacidad a sistemas puramente militares que no han evolucionado al ritmo frenético de las tecnologías civiles, debido al peso en la economía de escala de estas últimas.

La economía del dron también se conecta con un factor aún más importante: la industria militar tiene acceso a un pool de técnicos creativos y talentosos muy reducida en comparación con el sector civil, tanto empresarial como comunitario - open source. Si el empresarial ha sido decisivo para poner en servicio sistemas críticos, sobre todo de *hardware* exótico, capaz y barato (los *Systems on a Chip* que mueven los smartphones o los drones), el mundo open source aporta algo igualmente valioso, especialmente en los tiempos de una guerra existencial: miles de jóvenes, y no tan jóvenes, con talento y la máxima motivación posible.

A los jóvenes que han puesto en marcha decenas de grupos voluntarios primero, y ahora war startups, nadie les explicó que no se podía iterar en semanas y poner productos en servicio invirtiendo decenas de miles de dólares. Como no lo sabían, y como contaban con el conocimiento comunitario acumulado por sus predecesores en los distintos dominios, lo hicieron. Migraron los sistemas de Github¹⁴ a la guerra.

¹⁴ El mayor repositorio o almacén de software libre del mundo. Disponible en: www.github.com

12 War Startups, academias, iniciativas gubernamentales: reinventar la guerra para salvar la patria

En esta década, y con tal de tener acceso a internet, cualquier persona con un mínimo de talento y persistencia puede adquirir conocimientos sobre tecnología a un nivel inaudito. Todo el conocimiento necesario está disponible en una cantidad básicamente ilimitada de recursos de aprendizaje. Además, todos aprenden de todos, en el mundo del software libre las personas se saben parte de una cadena que aprende primero y enseña después.

Posiblemente uno de los factores más críticos para la supervivencia de Ucrania ha sido traducir este espíritu a amplios ámbitos de la defensa nacional. Es sabido que una parte importante de los desarrollos de hardware y software no se mantienen en secreto empresarial, sino que se comparten en un modo de comunidad open source abierta a todos los que pasan los filtros de seguridad pertinentes. La ventaja que proporciona este esquema es decisiva: el conocimiento adquirido y el software desarrollado se comparte para no reinventar la rueda y para trabajar a partir del arte previo, entendiéndose previo como aquello publicado hace más de 48 horas.

Sobre todo en el caso ucraniano, hay que señalar que han llevado el espíritu de las licencias libres del open source a su máxima expresión, de manera que cada innovación en software, en hardware, en combinatoria de componentes y en operativa, se difunde sobre todo en los espacios autorizados y, hasta donde se puede, en espacios cuya única puerta es hablar ucraniano.

En los mencionados artículos de la RGM y capítulo sobre drones del III libro de la guerra de Ucrania, se relata la transición del espíritu organizativo del Maidán a las organizaciones de voluntarios. En los primeros años, la carencia de medios impidió que madurara en Ucrania un ecosistema nacional como el mencionado. Pero la amenaza existencial y el apoyo interno y externo se combinaron para dar el paso de forma colectiva. Por ejemplo, a lo largo y ancho del país han surgido decenas de academias y pequeños centros de enseñanza en los que diseminar el conocimiento. Miles y miles de makers han adquirido en dichos centros, o simplemente por el boca a boca, conocimientos para seleccionar e integrar componentes en drones que respondan a distintas necesidades, y para reparar o canibalizar los drones dañados. Además, los veteranos de un rol particularmente peligroso vuelven del frente para formar a miles y miles de pilotos en el conjunto de habilidades que necesita un joven para trasladar su memoria muscular del gamepad de una consola a la emisora de un dron (como se explica, empleando simuladores civiles) y adquirir los también mencionados conocimientos y habilidades de fieldcraft para minimizar el riesgo al entrar y salir de posición.

Los grupos voluntarios han evolucionado con la guerra. Algunos han buscado apoyo financiero a través de la publicación de vídeos de todo tipo: sus creaciones, entrevistas, acciones exitosas, etc. Esto les ha generado un flujo constante de ayuda voluntaria, en especie y mediante servicios de donación tipo Patreon¹⁵. Al mismo tiempo, esta misma visibilidad les ha permitido lanzar eventos puntuales de *crowdfunding* para sufragar gastos extraordinarios, desde un 4 x 4 hasta cámaras infrarrojas. Esta actividad continuada en redes sociales, además, ha permitido al gran público conocer la guerra de los droneros contada por ellos mismos, y se puede afirmar que su contribución al mantenimiento de la visibilidad de la causa ucraniana ha sido significativa. De cualquier forma, la mayoría de ellos han cedido el testigo de la innovación tecnológica a las *war startups*, las empresas con fondos y recursos humanos para trabajar en los siguientes pasos evolutivos de los drones. Ahora mismo, el papel principal de los grupos voluntarios está tanto en las operaciones militares como en la construcción de distintos modelos de drones FPV, como sobre todo en la transmisión de sus conocimientos y experiencias de valor incalculable.

El siguiente paso evolutivo han sido las *war startups*. Hacia febrero de 2022 la industria de defensa ucraniana se encontraba en plena transición entre la industria heredada de la URSS y que perseveraba en adaptarse a la demanda del mercado internacional, por un lado, y un grupo creciente de pequeñas empresas rupturistas que hacían lo posible por mantenerse a flote, por otro, antes de esa fecha, la percepción de amenaza era muy limitada, y de ahí que no recibieran un apoyo suficiente del capital nacional o internacional o del propio Estado. Pese a eso, algunos de sus desarrollos en drones militares se unían a los desarrollos de los grupos de voluntarios como cimientos de lo que iba a venir.

Las *war startups* están destilando el conocimiento nacido de la experiencia de combate y de los requisitos de los combatientes y lo combinan con los recursos de los *hackers*, desarrolladores e ingenieros que están culminando la conversión en industria de guerra, como se decía antes. Si en la segunda guerra mundial el fabricante de automóviles o de maquinaria agrícola pasó a fabricar máquinas de guerra de todo tipo, ahora las compañías IT y de ingeniería electrónica y electromecánica están migrando sus esfuerzos al desarrollo de software que aumente las capacidades de otros sistemas militares y al desarrollo de un abanico de sistemas no tripulados que crece sin cesar.

Además de los más visibles UAS, existe un sector que finalmente toma velocidad de crucero: los UGV. Los vehículos terrestres no tripulados, hasta la guerra, eran sistemas de industria de defensa pura. Su desarrollo en todo el

¹⁵ La mayor plataforma de patronazgo del mundo. Los seguidores de un creador de contenidos, artista, personas afines a una causa... pueden donar la cantidad periódica que prefieran empleando la plataforma.

mundo ha sido más lento que el de los UAS por la dificultad que conlleva la navegación por distintos entornos terrestres. De hecho, se tenía a la industria rusa como una de las líderes mundiales, hasta que la guerra ha demostrado que sus flamantes blindados no tripulados eran la versión UGV de los pueblos de Potemkin¹⁶. Por más que la industria puramente militar rusa o ucraniana de UGV no haya acabado de despegar, pequeñas startups están haciendo lo que saben hacer mejor: ser ágiles y desarrollar sistemas simples y económicos para tareas que ahora se revelan esenciales: el transporte, suministro y evacuación de heridos en los últimos kilómetros antes de la línea de contacto. Hasta que los UAS de carga se adquieran en número suficiente, para determinadas posiciones defensivas estos vehículos salvan vidas.

Existen, además, los USV (*Unmanned Surface Vehicles*, buques no tripulados de superficie). Una de las mayores sorpresas tecnológicas de la guerra y esta vez carentes de precedentes. En la más pura línea *chimple*, se trata de diseños que posiblemente no lleven ni un año en pruebas. Completamente desconectados de la tendencia previa mundial en USV —navíos de mayor porte, en ocasiones opcionalmente tripulados y por supuesto *expenplex* y poco aptos para el uso en masa— estos sistemas han combinado la simplicidad con la comunicación satelital para lograr éxitos que habrían hecho las delicias de los integrantes de la 10.^a Flotiglia MAS original. Han protagonizado el éxito individual más apabullante de los sistemas no tripulados en la guerra, al derrotar a la mayor Armada del Mar Negro, y suponen por sí mismos otra caja de pandora más: la letalización de productos civiles aún más económicos es una amenaza para instalaciones litorales y aún buques en aguas marrones que necesita de respuesta urgente, sobre todo dado que está al alcance de actores no estatales.

Una de las reacciones más decididas en esta línea vino de fuera de Defensa. Concretamente, del Ministerio de Transformación Digital, con Mijailo Fedorov a la cabeza. Antes de la guerra habían impulsado iniciativas de alto impacto para la e-administración y el desarrollo digital del país. Pero a la hora de la verdad actuaron con decisión y rapidez. Tras sacar en tiempo récord los servicios digitales esenciales a una nube securizada en el exterior y apoyar al recepcionado de los servicios prestados por Palantir en esos momentos críticos, el Ministerio puso en marcha una serie de iniciativas, una detrás de otra, con las que apoyar sin descanso el crecimiento del ecosistema de drones (entre otros). Aprovechando las experiencias previas de su equipo en el Ministerio, las iniciativas de Fedorov facilitaron, entre otros:

- United24, la iniciativa de búsqueda de solidaridad internacional más importante. Dentro de ella destaca *Army of drones*, un llamado

¹⁶ Grigori Potemkin erigió pueblos falsos con fachadas elaboradas para impresionar a la emperatriz Catalina II durante su viaje por Crimea en 1787, ocultando la pobreza de la región.

a la solidaridad internacional focalizada en los drones, dirigida al gran público occidental y de gran éxito. Con figuras de talla mundial poniendo literalmente la cara, lograron que los drones simbolizaran la resistencia y el apoyo a la causa ucraniana

- People's drones, iniciativa para diseminar por todo el país el montaje de drones FPV.
- Brave1, clúster de war startups creado en conjunción con el Ministerio de Defensa y otros ministerios para apoyar multidimensionalmente la actividad y el crecimiento de las startups.

La suma de estos actores genera un ecosistema de innovación sin precedentes y que merece mucha atención, ahora y en el futuro. Hay que asumir que, de momento, falta una pieza importante: uno o varios campeones nacionales o aún midcaps que vehiculen toda esta ebullición creativa y la ayuden a escalar. Si las war startups están para quedarse y ahora mismo juegan un papel crítico en la carrera de innovación que ayuda a mantener a Ucrania en la guerra, también es cierto que presentan obvias limitaciones a la hora de escalar y maximizar la producción de sistemas físicos.

Evidentemente, una industria post-soviética tampoco es la solución salvo en los casos de más inmediata necesidad como la fabricación de munición de todo tipo. Por otra parte, no es inmediato ni baladí poner en marcha una o más plantas de fabricación enfocadas a un modelo productivo 4.0., donde la robótica, la sensorización, el mantenimiento predictivo y la gestión logística avanzada pueden lograr tanto producción como flexibilidad imposible para un modelo taylorista previo. Los recursos de los aliados europeos a este respecto están a la cabeza mundial y probablemente se den decisivas sinergias a no mucho tardar.

13 Modificaciones: materiales, frecuencias

Para fianziar, se hará una revisión de algunas de las últimas tendencias en el campo de los drones comerciales letalizados.

Por una parte, se extiende el uso de materiales alternativos a la fibra de carbono para la carcasa de los cuadricópteros. Hay que tener en cuenta que la fibra de carbono es un material de manipulación y corte complejos debido al entrelazamiento de las fibras. Esto impide la fabricación en talleres pequeños y de recursos limitados. Como quiera que la mayoría de los filamentos empleados para la impresión 3D no son aptos para los esfuerzos mecánicos que generan los drones FPV, los materiales alternativos que se están ensayando y empleando son:

- Policarbonatos de alta resistencia fabricados por inyección.
- Madera de balsa.
- Aluminio.

Cada uno presenta diferentes ventajas de cara al eco radar, al peso o la economía. Sin embargo, lo más importante en todos los casos es que permite aprovechar infraestructura industrial previa y asegurar que los armazones o frames de fibra de carbono nunca sean un cuello de botella para la fabricación. Además, los drones de FPV de mayor tamaño empleados (9 y 10 ") generan semejante empuje que convierten el aumento de peso comparado con la fibra de carbono en algo irrelevante.

Después están los radios. Como se ha venido indicando, su evolución reciente se ha acelerado. A fecha de marzo de 2024, grupos de hackers de ambos contendientes han avanzado mucho en la modificación del *firmware* ELRS, de manera que emisores y receptores pueden emplear bandas muy alejadas de las originales. Esto dificulta la detección empleando los escáneres más populares y, por lo tanto, baratos y simples, y saca de la ecuación a aquellos inhibidores no preparados para lidiar con las nuevas bandas.

Este desarrollo es un *stop-gap* a la espera de que maduren algunas de las distintas iniciativas de creación desde cero de radios y protocolos de control basadas en radio definida por software. El desafío es mayor que el *hacking* ELRS, pero a cambio el cielo (radioeléctrico) es el límite: por encima del límite de 433 MHz, cualquier frecuencia puede ser empleada para transmitir paquetes con el ancho de banda y la latencia que se necesita para el control de los drones.

Otro desarrollo que madura rápidamente es el de redes mesh completas o híbridas. Requieren de hardware más complejo, caro y pesado que los pocos gramos de un RX convencional de dron, pero a cambio permiten que muchos más drones (nodos en una red, en este caso) empleen las mismas bandas de frecuencia a la vez. De cara a mantener una latencia y alcance aceptables, se están probando arquitecturas de dron nodriza, por las cuales los drones en la zona de operaciones emplean una red mesh conectada al dron nodriza, quien a su vez retransmite el conjunto total de información a la estación de control en una arquitectura comparable a la antaño popular wifi-wimax. Eso sí, plantea la dificultad de que el derribo de un dron nodriza provocaría la pérdida de control del resto de la formación. Hay que señalar que no se trata de un enjambre al ser cada nodo de la red pilotado por un operador humano.

Para concluir, hasta la fecha los desarrollos más importantes de capacidades autónomas, ya se ha mencionado la navegación con GNSS denegado y la guía terminal autónoma. No hay información en abierto sobre un salto decisivo de capacidades y, además, hay que tener en cuenta que el aquí y el ahora necesita solución, y que miles de mentes enfocadas en ganarle la partida al contrario van a seguir dando más y mejores resultados que sistemas autónomos, caros, complejos y probablemente menos flexibles.

De la misma manera, los «drones antirradiación» que empleen como guía la emisión RF de los inhibidores, están cerca de su puesta en servicio. Se trata de un problema complejo cuando no se pueden emplear antenas suficientemente separadas; con todo, hay indicios suficientes como para dar por bueno un TRL6 o incluso 7, empleando antenas más ligeras y sencillas y discriminando por software. Cuando este tipo de efectores se pongan en servicio en número suficiente se producirá una vuelta de tuerca al actual equilibrio del campo de batalla, de consecuencias imposibles de prever.

14 Conclusión

La tozudez de los hechos masivos relacionados con los drones comerciales letalizados no deja alternativa a la hora de considerar su importancia actual y futura. No solo han venido para quedarse y seguir evolucionando, sino que ya se están empleando por zonas cada vez más amplias del mundo. La generalización de su uso va a traer un goteo incesante de nuevas lecciones aprendidas. Ahora mismo los estudiosos de la letalización de drones comerciales viven el sesgo de Ucrania, dado que es en esta desdichada guerra en la que ha explotado el uso de los DCL. Sin embargo, en otros entornos de guerra de todas las intensidades, grises y de seguridad no militar, los DCL y su doctrina de empleo van a variar sustancialmente. Por ejemplo, si sobre los cielos de Ucrania reinan los drones de carga de 7 a 10 “, en otros escenarios los drones más ligeros y pequeños tienen mucho que decir.

El ecosistema de fabricantes de sistemas C-UAS está en plena transformación. Se está abandonando la excesiva fijación en los drones comerciales tipo DJI y tratando de construir sistemas de sistemas, en muchos casos, basados en el protocolo Sapient. Todas las aportaciones van a sumar probabilidad de mitigación mientras se mantengan al día por separado y juntas, y el papel del integrador va a ser crítico durante mucho tiempo.

Cada vez que el autor ha tenido la oportunidad, se ha mostrado optimista respecto a las posibilidades de la industria española de cara a alcanzar la primacía en este sector. Al ecosistema industrial y tecnológico a todos los niveles, desde las startups a las PYMES veteranas y midcaps se unen los campeones nacionales y todos ellos se pueden desarrollar en el conjunto único de espacios disponibles en territorio nacional.

Desde las instalaciones del INTA, pasando por los campos de maniobras, hasta llegar a la amplia variedad de espacios disponibles en la España vaciada, dentro de los límites que marca la normativa para pruebas, se dispone de una ventana de oportunidad que puede mantenerse abierta algunos semestres para situar al ecosistema español a la vanguardia de Europa. Cabe ser optimista y confiar en que las decisiones se tomen a todos los niveles y en los tiempos y las formas adecuadas.

Bibliografía

- Chulilla Cano, J. L. (2023). Presente y futuro de los drones comerciales letalizados. *Revista General de Marina*. 284, p. 4.
- Chulilla Cano, J. L., Román, J. F. y Villanueva, C. (2024). La guerra de drones en Ucrania. En: Murillo, B. C., López, C. D. V. y Piella, G. C. *La guerra de Ucrania III: De la reconquista de Jersón al estancamiento*. Los Libros de la Catarata.
- In Ukraine flight controllers for drones have been developed. (2024). *Revista Militarnyi*. [Consulta: 2024]. Disponible en: <https://mil.in.ua/en/news/in-ukraine-flight-controllers-for-drones-have-been-developed/>
- Kaldor, M. (1983). *The Baroque Arsenal*. Londres. Abacus.
- Murillo, B. C., López, C. D. V. y Piella, G. C. (2024). *La guerra de Ucrania III: De la reconquista de Jersón al estancamiento*. Los Libros de la Catarata.
- Suleiman, A y Hezaber, H. (2024) *The Syrian regime is stepping up its use of suicide drones* [en línea]. Al-Jazeera. [Consulta: 2024]. Disponible en: <https://twitter.com/SAMSyria0/status/1758174017855389802>
- Taylor, C. (2024). *Preparing to Win the First Fight of the Next War*. Modern War Institute at West Point.
- Watling, J. y Reynolds, N. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *Royal United Services Institute for Defense and Security Studies*. 19, pp. 18-20.