

Conversaciones sobre defensa aérea, y mando y control aéreo



JUAN JOSÉ RUIZ CENTENO
Coronel del Ejército del Aire
y del Espacio

Un verano cualquiera debajo de una sombrilla, en una de las hermosas playas gaditanas, conversa un oficial del EA con amplia experiencia en los temas de defensa aérea y mando y control aéreo y un familiar, profesional de alta dirección, y muy interesado en la transformación de las organizaciones.

—No sé si estarás al tanto de las noticias de Ucrania. Supongo y espero que los militares estaréis tomando buena nota.

—Fermín, supones muy bien. La verdad es que hay numerosos campos en los que habría que tomar nota, desde el diferente modo de afrontar determinados aspectos de un conflicto armado hasta el concepto del propio conflicto. Date cuenta que parece una guerra casi convencional, de las de antes, pero con tecnologías del siglo XXI. Yo, por deformación profesional, intento fijarme en todo lo que se refiere a la defensa aérea y el mando y control aéreo.

—¿Y eso qué es?

—Bueno, el concepto es complejo, pero te lo resumo de forma sencilla: los medios, sistemas, personas, estructuras o procesos para que los comandantes militares puedan conducir la guerra aérea. Es decir, la manera de enlazar aeronaves entre ellas, con el jefe y con otros sistemas de armas.

—Ya, pero eso estará muy asentado, digo yo

—Pues sí. Pero precisamente una de las lecciones de esta guerra podría ser que conviene ir pensando en cambiar algunos conceptos.

—A ver, explícate.

—Tradicionalmente el mando y control aéreo ha estado basado en estructuras jerarquizadas muy formales, en procesos muy bien definidos,

en redes centralizadas. A ver si me explico. Imagínate unas instalaciones con una seguridad y vigilancia muy estrecha, donde hay un núcleo principal, tipo búnker, desde el cual se dirigen todas las operaciones aéreas. Este concepto parece que podría dejar de servir tal y como lo conocemos.



El operador del presente



El operador del futuro

—¿Por qué no? En todas las películas americanas aparecen esas salas llenas de hileras de ordenadores y generales, donde se juntan los protagonistas a tomar las decisiones. Pero si algunos tienen hasta habitaciones y cocinas...

—Efectivamente este era el concepto. Y de hecho todavía es así en muchos sitios, y sigue habiendo gente que piensa que es el mejor modelo. Pero claro, el concepto manejado hasta ahora se basaba en que tu cen-

tro de operaciones era intocable, lo cual se ha comprobado que no.

—Bueno, es que para eso es un bunker.

—Sí, y por eso hay armamento anti-bunker. Seamos sinceros; hoy en día, creo yo, es un riesgo altísimo basar tu centro de mando en un sitio concreto, aunque sea «bunkerizado» y en un sistema informático único. Eso se acabó hace décadas. Siempre se designan lugares alternativos, pero no, por muy protegido que esté, siempre habrá alguna vulnerabilidad. En la actualidad, con el tema de la ciberguerra, todavía más. Hay un concepto muy utilizado cuando hablas con militares, que es el de centro de gravedad. Simplificando, eso que si le destruyes al enemigo, ganas la guerra o si te lo destruyen, la pierdes. Y todo lo que se relaciona con el mando y control suele figurar en la lista de los posibles centros de gravedad, que hay que identificar, localizar y destruir.



Enjambre de drones y sistema de combate



Sistema radar embarcado JLENS de Raytheon

—Pero entonces, ¿cuál es la solución? Porque ya me dirás cómo proteges ese mando y control.

—Bueno, dividamos:

Por un lado, están los sensores que se usan para proporcionar información a ese sistema de mando y control aéreo. Tradicionalmente, los radares. De hecho siguen siendo la piedra angular para saber qué vuela en tu espacio aéreo. Y dentro de los radares, simplificando mucho, hay tres tecnologías en relación con su disposición geográfica: los fijos, los móviles y los aéreo-embarcados. Los más utilizados son los fijos, pero tienen una clarísima desventaja: todo el mundo sabe dónde están y por tanto son fáciles de eliminar.

—Bueno, todo el mundo...

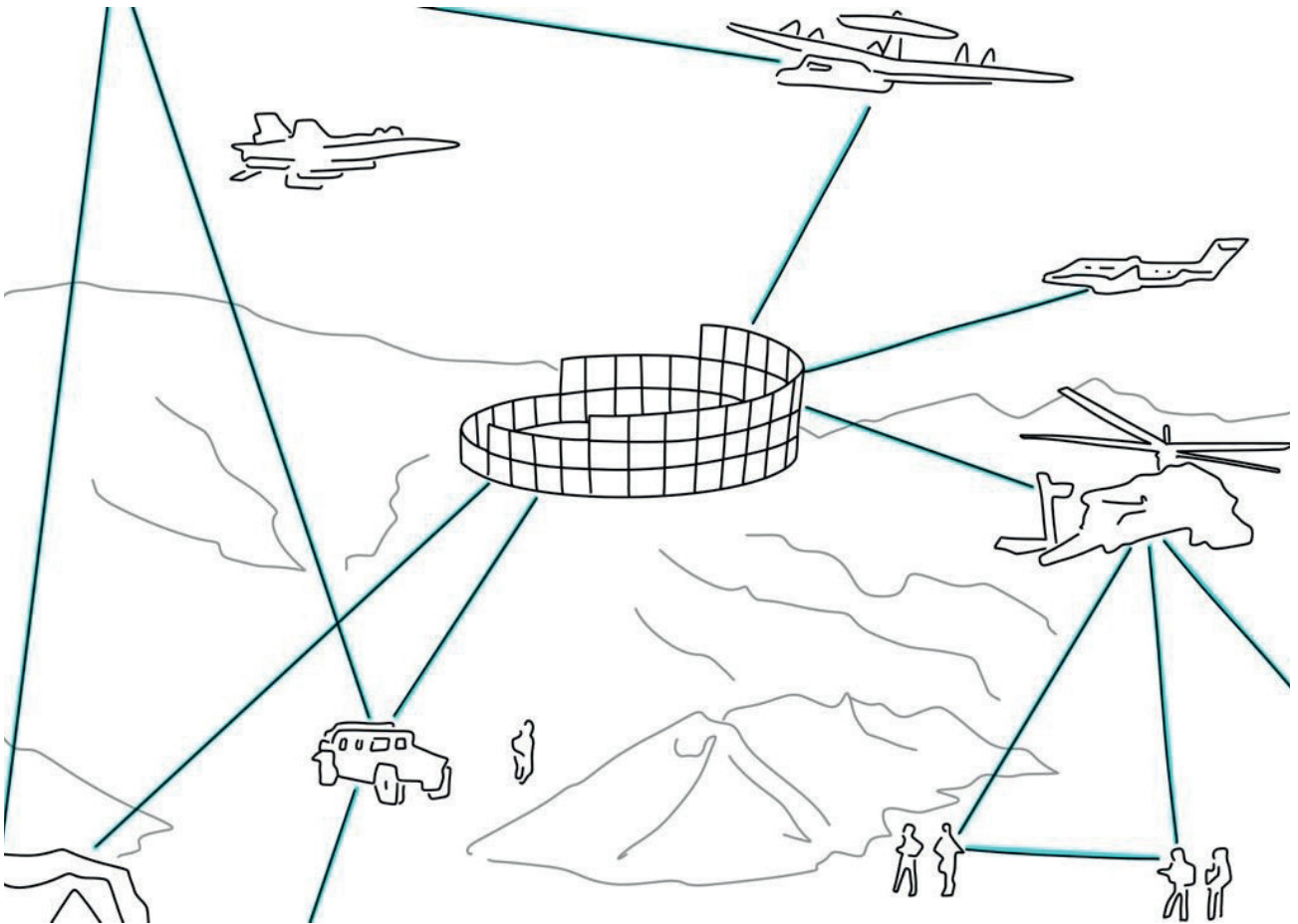
—Pues sí, suelen ser aparatosos, estar en lo alto de montes y con unos radomos (protegen al radar de la meteorología adversa) que les hace fácilmente identificables. Búscalos en Google Maps y verás. En la práctica los puedes defender con artillería antiaérea pero hay muchas otras amenazas. Algunas muy baratas, como drones o sabotajes. En todas las guerras convencionales suele ser lo primero que se destruye.

Después tenemos los radares móviles o transportables, que como dice su nombre los puedes mover de ubicación con camiones o aviones y puede ser interesante contar con el mayor número de ellos. Pero requieren mucho personal y medios, que habitualmente no se tienen.

Y por último los aéreo-embarcados, ya sea en aviones, como en AWACS, en drones o incluso en globos o dirigibles. Por ejemplo en algunos teatros de operaciones dedicados ya se utilizan estos últimos. Todos estos podrían ser menos vulnerables pero suelen ser muy caros de adquirir y operar.

—¿Y cómo se soluciona el tema de los sensores?

—No es fácil. Quizás la solución sea contar con un número adecuado de



La nube de combate

diferentes tipos y plataformas de radar, incluidas aquellas que operan desde el espacio o desde plataformas a gran altitud llamadas HAPS o pseudo satélites. El espacio, nuestro nuevo ámbito de actuación, será fundamental. Pero sobre todo explorando nuevas tecnologías como los sensores pasivos, que son manejables y más baratos. El problema es que la precisión es menor, pero la tecnología está evolucionando mucho y gracias sobre todo a las capacidades de computación y a la inteligencia artificial, estoy seguro que podrá ser una solución. En cualquier caso, lo que tienes que entender es que los sensores lo único que proporcionan al sistema es información. Y que si bien ahora tenemos en mente al radar como origen estrella de esa información, estoy seguro

Hoy en día se tiende al concepto de arquitecturas orientadas a servicios, donde tiene especial importancia la red, la nube, y donde a los programas se accede directamente en la web, usando el propio explorador

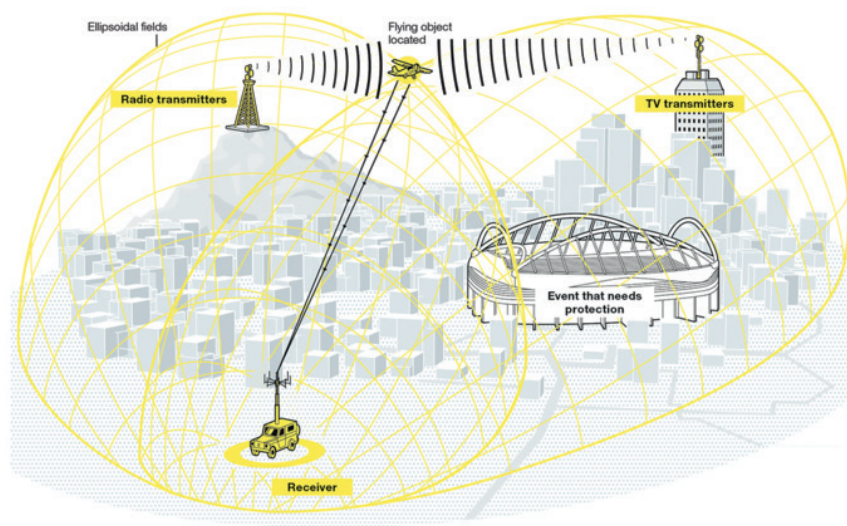
que en el futuro esa información vendrá de muchas y muy diversas fuentes.

—Vale, entendido el tema sensores, pero en cuanto a los centros de mando, ¿cuál es la solución?

—Pasa un poco como con los radares. Hay que asumir que nuestros potenciales enemigos conocen la ubicación exacta de nuestros centros de mando. También hay que asumir que la defensa física de estos centros, por muy búnkerizados que estén, puede ser difícil, si no imposible. Hay armamento diseñado precisamente para ello.

Por eso cobra mucha importancia la opción de la dispersión geográfica. En la práctica, e idealmente, sería tener a todo el personal que tiene alguna función en ese centro de mando, disperso en diferentes ubicaciones.

Eso requiere un cambio tecnológico importante y por supuesto una evolución en la forma de operar y, sobre todo, un cambio de mentalidad.



Sistema de radar pasivo

En cuanto al cambio tecnológico, hasta ahora los sistemas informáticos que se han utilizado para el planeamiento y ejecución de operaciones aéreas eran sistemas muy específicos, con *hardware*, servidores y consolas, diseñados *ad-hoc* para estas tareas. Fíjate que hasta existían lenguajes de programación específicos para ello. Esto, obviamente implicaba grandes salas de servidores, con sus sistemas de energía y climatización, consolas como las de las películas, etcétera.

Pero hoy en día se tiende al concepto de arquitecturas orientadas a servicios, donde tiene especial importancia la red, la nube, y donde a los programas se accede directamente en la web, usando el propio explorador. Ya hay fuerzas aéreas que tienen así sus sistemas.

—Pero, hombre, ¿cómo vas a utilizar internet para eso! Es una locura y los hackers terminarían impidiendo su uso

—He hablado de la red o de la web, pero no me refiero a internet. Son redes privadas, que en muchos casos no utilizan absolutamente ningún servicio que no sea militar. Es decir que todas las líneas de telecomunicaciones, ya sean cables, fibra óptica, o sobre todo satélites, son militares. Se trata de redes que no tienen nin-

gún tipo de conexión física con internet para que nadie que esté fuera de la red privada pueda entrar. E incluso utilizando servicios no militares, es decir contratando empresas para proporcionar alguno en concreto, existen formas de cifrar los datos...

—Sensores y centros de mando comprendidos, pero ¿hay algo más?

Interoperabilidad y conectividad son conceptos clave para que los sistemas de mando y control sean efectivos

—Nos quedan los sistemas de armas, lo que en algunos textos definen como efectores, que no dejan de ser los que al final llevan a cabo la misión. Normalmente aeronaves, cazas, aviones de transporte o helicópteros, pero cada vez más aeronaves no tripuladas, misiles de crucero, etc. Claramente forman parte del sistema y cada vez con más conectividad y capacidad. De hecho los llamados cazas de quinta generación, los más modernos, son ya nodos inteligentes con una altísima capacidad no solo

de ejecutar la misión sino de llevar a cabo otras funciones de mando y control como coordinación, asignación de misiones y armamento, etc.

—Por lo que has dicho, al final esto del mando y control se resume en ser capaces de conectar muchas cosas y que estas se entiendan.

—Sí, eso lo conocemos como interoperabilidad y conectividad, y efectivamente son conceptos clave para que los sistemas de mando y control sean efectivos. Hoy en día mucho más, porque cada vez habrá más sensores de todo tipo, más plataformas y más elementos que deben formar parte del sistema. Pero claro, con el cambio tecnológico se debe llevar a cabo también un cambio en las estructuras, procesos y procedimientos para aprovechar estos avances de la ciencia. Entiende que de nada serviría que todo el mundo estuviera perfectamente conectado y compartiendo información en tiempo real, y siguiésemos utilizando estructuras y procesos inventados en los años cincuenta del siglo pasado, cuando como mucho se usaba un teléfono e intercambios de datos muy limitados.

—Oye, y eso de los drones, ¿también afecta?

—Pues ese es un tema crucial. No solo por las capacidades que nos dan, sino porque pese a ser no tripulados o incluso autónomos, hay que integrarlos con el resto de aeronaves y plataformas. Hablamos de gestión de espacio aéreo, órdenes de misión, planes de comunicaciones, etc. Pero también está el aspecto de la defensa contra drones, lo que conocemos como C-UAS o contra UAS, que como se ha visto en Ucrania, suponen una amenaza creciente y para la que hay que estar preparados. Eso requiere otro tipo de sensores, otro tipo de procedimientos, algo que hasta ahora no se había previsto, pero en lo que ya se está trabajando.

—Y esto de la inteligencia artificial que has mencionado antes, ¿afectará?



—Como en todo. La inteligencia artificial va a revolucionar nuestra sociedad y cómo vivimos. Y por supuesto también lo militar, y dentro de esto, el mando y control aéreo. Hay multitud de aplicaciones en las que la inteligencia artificial puede tener cabida; desde las más ambiciosas como el desarrollo de estrategias o planes operacionales hasta las más técnicas o tácticas, como la identificación y seguimiento automático de blancos, hasta el diseño de planes de telecomunicaciones o asignación de frecuencias; diseño de planes de espacio aéreo, creación de ATO, que son nuestras órdenes tácticas, etcétera. Las posibles aplicaciones son casi infinitas.

—Pues parece buena idea usar esta nueva tecnología, ¿no?

—Por supuesto, es una oportunidad. Pero también un reto por los riesgos que puede acarrear. Por ejemplo, la inteligencia artificial se nutre de aprendizaje, lo que se conoce como machine learning. Y evidentemente dentro de este aprendizaje, los datos e información con los que se va

a alimentar a esta inteligencia artificial deben ser cuidadosamente seleccionados. Tiene que «aprender», si se permite la expresión, nuestra doctrina, procedimientos e incluso nuestra cultura y valores. Claro que cuanto más información, mejor, pero no todo debe «enseñarse». Imagina que enseñas falsedades; entonces lo que «aprende» será falso. Es decir, no vale un ChatGPT público, hay que crear herramientas propias alimentadas internamente por nuestra organización. Además, hay decisiones militares que no deberían «delegarse» en una inteligencia artificial, sobre todo las relacionadas con el uso de la fuerza. Y por último, todavía habría que estudiar los sesgos de aquel personal más habituado a depender de la inteligencia artificial. Se han hecho estudios preliminares que parecen indicar que hasta cierto punto se pierde libertad de pensamiento, o imaginación, o simplemente creatividad. Y ¡jojo! no olvides, Fermín, que lo militar es una ciencia, pero también un arte, que por tanto requiere de esas características del ser humano.

—Y de todo lo referente al mando y control, ¿qué es el componente que consideras más importante, más crítico?

—Sin duda las personas. Te habrás dado cuenta las complejidades tecnológicas y los cambios vertiginosos que experimenta este campo. Pues detrás de todo ello debes tener profesionales muy cualificados, comprometidos y con una mentalidad abierta a nuevas formas de trabajar. Todo lo que te he contado requiere de un equilibrio entre tradición, experiencia o rigor, y capacidades un tanto disruptivas como el ingenio, la creatividad, la imaginación, o la astucia, por poner algunos ejemplos.

—¿Pero tenemos a estas personas tan especiales?

—Decía Jim Collins «Las personas no son el mejor activo de una organización; las personas adecuadas son el activo más importante de una organización». Y el Ejército del Aire y del Espacio está formado por ellas, de lo cual nos sentimos satisfechos todos los que pertenecemos a él. ■