COMBATE en las ondas

El espectro electromagnético es el campo de batalla del Regimiento de Guerra Electrónica 31

UN convoy avanza por un camino en Afganistán. En él va un todoterreno con un equipo de guerra electrónica. El operador capta una conversación del enemigo por *walkie talkie*. El intérprete que está a su lado la traduce. Inmediatamente, se lanza la alerta: «¡Mi capitán! en un minuto nos hostigarán por el oeste». El mando ordena replegarse. Han dado la vuelta a la situación y ahora llevan la iniciativa. Son circunstancias que conocen muy bien los sargentos primeros Díaz y Ballesteros. «Al saber lo que iban a hacer, podíamos anular el efecto sorpresa de un ataque enemigo», señalan estos dos militares del Regimiento de Guerra Electrónica 31 (REW 31), perteneciente al Mando de Transmisiones del Ejército de Tierra.

Desde su creación, en 1996, esta unidad ha enviado a sus hombres y mujeres a los distintos escenarios y zonas de operaciones de todo el mundo donde ha sido requerida su presencia. Son militares muy especializados, en continuo proceso de adaptación a las técnicas emergentes en este campo. Si la tecnología militar ha avanzado a pasos de gigante, el salto de las comunicaciones ha roto esquemas al pasar del uso de palomas mensajeras a la guerra electrónica (*electronic warfare* o EW), fundamental en todos los dominios del combate: tierra, mar, aire, espacio y ciberespacio.

Su campo de actuación son las ondas electromagnéticas. Un ejemplo es el radar, que empezó a funcionar como arma defensiva en la II Guerra Mundial para detectar aviones enemigos. Pero el campo de la EW se ha ampliado hasta extremos casi inimaginables,

Los equipos del REW 31 están instalados sobre vehículos y *shelters* de varios tipos.

algo que se palpa al adentrarse en las dependencias del acuartelamiento *Zarco del Valle*, en el madrileño barrio de El Pardo, sede del REW 31. Sus pabellones, construidos en 1917, encierran algunas de las tecnologías más punteras del Ejército de Tierra. De hecho, el nombre del cuartel da pistas del espíritu que lo impregna. Antonio Remón Zarco del Valle y Huet (1785-1866) fue un general y ministro de la guerra que, además de ser condecorado cuando era capitán de ingenieros en la guerra de la Independencia, fue presidente de la Real Academia de Ciencias y miembro de otras 23 academias y sociedades científicas, algunas en el extranjero.

El avance tecnológico es fundamental porque el combate no lo gana quien más bombas lanza sino quien mejor las dirige y más evita, y esto es una misión básica de la EW. Situaciones como las que vivieron nuestros soldados en Afganistán son buena muestra de ello, pero pueden ser de lo más variadas, como otra que relata el suboficial mayor J. Carlos Pinilla Robledillo: Cuando un convoy atravesaba una población el equipo de EW detectaba actividad de telefonía. «Era algo normal; la gente habla por teléfono». Pero, como describe Pinilla: «Si al salir hacia la carretera la actividad móvil desaparecía pero aumentaba de nuevo a varios kilómetros, en medio de la nada, había que estar prevenidos; podría ser que quisieran activar un explosivo por telefonía móvil. En estos casos, el operador de EW advierte al mando del convoy y este despliega a sus hombres y hace volar drones de vigilancia para saber lo que está pasando».

DE SALVACIÓN A PESADILLA

Es decir, los equipos de guerra electrónica salvan vidas, pero también son una potente arma ofensiva. El coronel Francisco Javier Fernández Conde, jefe del REW 31, pone como ejemplo el ataque de Zelenopillya, en la guerra del Donbás, en julio de 2014: «Los rusos localizaron un batallón mecanizado gracias a las comunicaciones que emitía. Lo confirmaron por otras fuentes y lanzaron un ataque con cohetes desde quince kilómetros de distancia. El batallón quedó aniquilado. Los ucranianos se dieron cuenta de que habían sido localizados por sus comunicaciones, así que las redujeron al máximo, pero esto provocó descoordinación en sus movimientos».

El equipamiento electrónico con el que opera la unidad puede interceptar comunicaciones de radio, imagen o *data link*.

En el ensayo *The Kill Chain*, sobre guerra electrónica, se describe otro caso muy ilustrativo, el de unos *hackers* rusos que engañaron a un comandante ucraniano para que respondiera a una llamada de móvil que parecía de su madre. Al descolgar, lo geolocalizaron y lo mataron con cohetes de precisión. Y es que, como apunta el coronel Fernández Conde, la guerra electrónica ofrece muchas posibilidades: «Por ejemplo, meter ecos falsos en el radar enemigo para hacerle creer que hay algo, o simular comunicaciones en un punto para que el adversario piense que allí se ha establecido un puesto de mando».

Los equipos de guerra electrónica salvan vidas, pero también son una potente arma ofensiva

Otra de sus aplicaciones es la *guerra de navegación*. «Consiste en degradar la señal de los satélites sobre geoposicionamiento de buques y aviones. Es lo que se llama *spoofing*, anular o alterar la señal de GPS. Se puede modificar, incluso, la de un misil guiado por GPS», señala el coronel. Su efecto puede ser decisivo en el combate aéreo: «¿Se imagina un caza volando a 900 km/h y que el piloto no sepa dónde está porque su GPS le da una posición errónea? A partir de aquí los errores van en cadena: abrir fuego amigo, no encontrar avión nodriza para abastecimiento, etcétera». Quién sabe si por eso algunos de los cazas rusos derribados en la guerra de Ucrania llevaban GPS básicos pegados a los tableros: no se fiaban de donde estaban.

Aquí es donde entran en juego las contramedidas de guerra electrónica. La más conocida de aviones y helicópteros son los *chaff* (del inglés, señuelo). Se trata de soltar una nube de pequeñas piezas de aluminio, fibra de vidrio o plástico metalizado. Cuanto más ligeras más tiempo permanecen en el aire. Lo que generan en el radar es una nube electromagnética que le impide ver dando tiempo al piloto a una maniobra evasiva. Pero contra esta contramedida hay otra medida: la inteligencia

artificial, la tecnología que acumula millones de datos de comportamiento para, a partir de ahí, sacar patrones de conducta. Mediante ella, el misil puede anticiparse a la maniobra evasiva por la que optará el piloto.

Poco se puede hacer también contra las microondas de alta potencia. «Se trata de ondas electromagnéticas de alta frecuencia que no provocan explosiones como un fuego de artillería pero que, literalmente, pueden *freír* los circuitos al ser alcanzados por una intensísima descarga», señala el coronel Fernández Conde. En un principio, no afectarían a los humanos aunque hay dudas: ahí están los ataques a embajadas de EEUU en Cuba o en China en las que los funcionarios se quejaban de fuertes dolores de cabeza. En cualquier caso, si la descarga alcanzara un avión se iría abajo.

En Estados Unidos cuentan con el sistema de respuesta operacional táctica de alta potencia THOR (*Tactical High Power Operational Responder*), capaz de tirar abajo enjambres de drones atacantes. En España también existe un escudo antidrones; se llama sistema ARMS y lo ha desarrollado Indra. Y es que, según el coronel Fernández Conde, España está entre los cinco primeros países en desarrollo de sistemas de guerra electrónica. De hecho, es un motor de la industria tecnológica de nuestro país. Por ejemplo, recientemente Indra presentó *Elint,* un sistema portátil de EW que cabe en una mochila.

El personal de la unidad está en continua formación, acorde con los rápidos avances tecnológicos y de los medios empleados en sus misiones.

Volviendo a la detección de drones, el jefe del REW 31 describe el sistema *Cervus* que utiliza el Ejército de Tierra en sus misiones: «identifica por donde viene el dron, si puede llevar explosivos o si solo capta imágenes. A partir de ahí, podemos hacerlo caer al suelo o asumir su control y llevarlo adonde queramos, por si porta una bomba, o hacerlo volver al punto de origen».

La Compañía de Ciberdefensa del REW 31, creada en 2018, es responsable de la seguridad informática de las unidades del Ejército en campaña.

CIBERDEFENSA TÁCTICA

En un campo de batalla los mandos rara vez salen de la tienda de campaña para otear el horizonte con unos prismáticos. Permanecen dentro, rodeados de ordenadores. Son sus ojos. Ahí tienen la información. Pero, ¿y si les entra un virus? De que eso no suceda se encarga la Compañía de Ciberdefensa del REW 31, responsable de la seguridad informática cuando es requerida en ejercicios y maniobras, dentro y fuera de España —no así de las redes fijas, que es tarea del Mando Conjunto del Ciberespacio—. La Compañía de Ciberdefensa del REW 31 puede enviar a la zona de operaciones de cuatro a ocho personas, perfectamente identificables por las voluminosas maletas negras en las que llevan sus equipos informáticos. Continuamente analizan líneas en la pantalla que, para el resto de los mortales no tienen ningún sentido, pero que pueden contener todo tipo de *malware*.

Gabriel Cruz
Fotos: Pepe Díaz