1.4

La guerra electrónica y ciberguerra en el conflicto de Nagorno–Karabaj en el contexto del empleo de drones como multiplicador de fuerza

Por el CR Com (R) Ing Mil Rafael Mario Olivieri

Temario

PALABRAS CLAVE: Nagorno Karabaj, Armenia Azerbaiyán, guerra electrónica, EW, espectro electromagnético, ciberguerra, loitering munitions.

Introducción

La rápida y contundente victoria de Azerbaiyán, caracterizada por el empleo de nuevas tecnologías en el campo de batalla, que ya eran conocidas, pero que en este caso se emplean por primera vez en un conflicto del tipo Estado contra otro Estado ha despertado un gran interés entre los analistas militares y las naciones sobre las lecciones de este conflicto para futuras guerras.

En particular, el desgaste de las defensas aéreas, la artillería y vehículos blindados armenios por *vehículos aéreos no tripulados* azeríes, el uso de fuego de artillería dirigido por estas plataformas y el uso de munición guiada, entre otras, ha llevado a un debate significativo sobre los recursos del poder militar en operaciones militares de alta intensidad.

Pero detrás de las consecuencias visibles del fuego y la maniobra existen otros recursos que desarrollan acciones en otro espacio que no es el campo de combate definido en la tierra, el cielo o el mar: *la guerra electrónica y la ciberguerra*. Se demuestra que sin el dominio en estos espacios, no será posible el dominio en el campo de batalla real, por mas que se cuente con superioridad de medios.

La guerra electrónica – EW (electronic warfare)

La *guerra electrónica* es una actividad que se desarrolla en un espacio intangible denominado espectro electromagnético, que podemos definir, en una apretada síntesis, como el conjunto de todas las frecuencias posibles que producen radiación electromagnética. No todas las ondas electromagnéticas tienen el mismo comportamiento, por ello el espectro electromagnético se divide convencionalmente en segmentos o bandas de frecuencia. De la misma forma, el empleo militar de este espacio es diverso: para comunicaciones, que posibilitan el comando y control y "no comunicaciones" o uso en sistemas de armas y sensores.

Este espacio no se puede delimitar de la misma forma que el campo de combate mediante líneas o límites en el terreno, puesto que las ondas electromagnéticas no se ajustan a ellos, sino que se propagan en el espacio real conforme a leyes de la física, dependiendo de su frecuencia, potencia, direccionalidad de la radiación y condiciones meteorológicas, entre otros.

El dominio de este espacio es crucial en la guerra moderna, puesto que por él se comunican y comandan las fuerzas en el terreno (Comando y Control). Los sensores pueden detectar amenazas a tiempo, y se pueden guiar sistemas de apoyo de fuego, para citar algunos ejemplos.

La guerra electrónica incluye acciones defensivas, para asegurar el uso propio del espectro electromagnético por parte de la propia fuerza, y acciones ofensivas, tendientes a obtener información y negar al enemigo el uso de su espacio electromagnético, con lo cual afecta su comando y control, y reduce y/o neutraliza su uso por parte de distintos sistemas de armas. Además, es una valiosa fuente de reunión de información de inteligencia.

La ciberguerra

Al igual que el concepto anterior, la *ciberguerra* se desarrolla en un espacio intangible, denominado ciberespacio. Tampoco podemos definir sus límites físicos, aunque potencialmente abarca todos los sistemas de comando y control y sistemas de armas conectados en red que emplean software.

Se puede "entrar" a ese espacio por medio de las redes de datos, en muchos casos desplegadas en el espectro electromagnético, pero hay mas formas, en general basadas en el engaño, y en la explotación de vulnerabilidades técnicas y humanas, convirtiéndolo en un espacio muy complejo.

Los sistemas actuales de comando y control, y sistemas de armas integran componentes electrónicos avanzados, que incluyen software embebido en ellos, integrados a los sistemas de información para lograr capacidades avanzadas. La evolución tecnológica de los sistemas de armas y de comando y control hace necesario el uso del ciberespacio, ganando capacidades, pero a la vez exponiendo vulnerabilidades.

La ciberguerra, al igual que la guerra electrónica, incluye acciones defensivas, para proteger del enemigo los sistemas de información y sistemas embebidos propios, y acciones ofensivas,

para negar / neutralizar su uso por parte del enemigo, y constituye una importante fuente de información de inteligencia. Se extiende a Internet y redes sociales, y también es una plataforma para operaciones de guerra psicológica.

La *ciberguerra* desarrolla acciones que se pueden percibir en forma directa, por sus resultados, como la negación de un servicio, pero también otras imperceptibles, muy peligrosas, con consecuencias muy variadas.

El conocimiento

Si bien operar en el espectro electromagnético o el ciberespacio, requiere de equipamiento, no será posible su empleo exitoso, sin el personal calificado y entrenado.

En países que lideran estos conceptos, como en las Fuerzas de Defensa de Israel, vemos a personal calificado en estas operaciones, por ejemplo personal con estudios en ciencias exactas o ingeniería, que son los mejores operadores de estos sistemas, porque no se ajustan solo a procedimientos establecidos, sino que desarrollan su actividad en forma proactiva, y pueden planificar y desarrollar acciones para situaciones especiales, aplicando sus conocimientos e iniciativa.

Además, el conocimiento de la ciencia y la tecnología que se puede aplicar a la solución de un problema militar, permite realimentar al sistema, adecuando doctrinas y generando recursos innovadores, muchas veces disruptivos que permiten obtener la ventaja en el campo de combate.

El conflicto de Nagorno – Karbajh

Armenia se había preparado durante mucho tiempo para un ataque de Azerbaiyán con el objetivo de recuperar la tierra perdida en el conflicto de 1994, pero esperaba una guerra de maniobras convencional y confiaba en su capacidad de maniobra, basada en vehículos blindados, y en su potencia de fuego, con cañones, obuses y misiles, junto con su poder aéreo, incluyendo medios avanzados de defensa aérea. En cambio, el combate real fue contra un adversario que tenía un alcance extendido, que podía atacar donde quería y que desarrolló una guerra de desgaste, hasta doblegar su capacidad de defensa. ¿Cómo logró esto Azerbaiyán? Tomo la iniciativa en el empleo de la tecnología. Los analistas coinciden en el acertado empleo de drones y hasta se vieron algunas acciones de *ciberguerra* en redes sociales.

Sistemas de defensa aérea armenios, incluidos los complejos TOR y S-300 de origen ruso fueron vulnerables. Más de 30 sistemas de defensa aérea armenios fueron destruidos por drones turcos TB2 armados con inhibidores electrónicos y micro munición (MAM), similares a los sistemas Hellfire, así como por drones israelíes merodeadores Harop, Orbiter-1, y por drones kamikaze turcos Kargu. Azerbaiyán ganó el espacio aéreo. Estos sistemas de armas inmobilizaron a las fuerzas terrestres armenias. Al mismo tiempo, YouTube fue el medio elegido para publicar los videos azerbaiyanos de ataques exitosos con drones, lo que provocó un gran impacto psicológico que afectó la voluntad de lucha de su enemigo. Armenia, si bien contaba con alguna tecnología propia de drones, no llegó equiparar a su oponente.

Azerbaiyán consiguió dominar y derrotar a las fuerzas armenias empleando nuevas tecnologías y doctrina.

Estas nuevas tecnologías y armas desarrollan su poder empleando el *espectro electromagnético y el ciberespacio*, cuestiones que sin duda Azerbaiyán tuvo en cuenta. La sorpresa no fue tanta, Azerbaiyán ya había exhibido parte de su arsenal en desfiles militares y videos, y Armenia contaba con sistemas de guerra electrónica, pero no fueron lo suficientemente efectivos como para neutralizar los ataques de su enemigo. No podemos saber aún si fue por deficiencias de esos sistemas o por falencias en su operación y empleo.

Los drones aparecen cada vez mas en la oferta de material bélico de muchos fabricantes desde hace unos años a esta parte, y ciertamente han demostrado su eficacia y ventajas en este conflicto.

Son redundantes, más baratos que las aeronaves tripuladas, pueden soportar regímenes de vuelo que son demasiado complejos para los pilotos humanos, operan con cierta autonomía con poca intervención humana, y han demostrado una y otra vez que son multiplicadores de fuerza. Funcionan como una *alternativa asimétrica* frente a costosos y complejos sistemas de armas y permiten el dominio del campo de combate combinado con adecuados sistemas de armas, como artillería, proyectiles guiados, cohetes y misiles. Si algún sistema de armas se destacó en forma contundente en este conflicto, es sin duda este.

¿Dónde y cómo interviene el espectro electromagnético y el ciberespacio?

Dicho todo esto, entramos en el objeto de este trabajo, que nos permite ver las fortalezas y debilidades de estos sistemas, cómo funcionan en el ataque u obtención de sus objetivos, y qué recursos emplea quien se defiende de sus acciones.

Un vehículo no tripulado de combate aéreo UCAV *(unmanned combat air vehicle)*, mas conocido a nivel popular como *drone* o *dron de combate*, es una aeronave no tripulada o UAV *(unmanned aerial vehicle)* diseñado para empleo militar, con armamento o no, según la función que desempeñe. No tienen piloto humano a bordo, y las misiones de los drones se realizan generalmente bajo el control humano en tiempo real desde una estación de control, aunque algunos pueden hacerlo en forma autónoma.

La tecnología de los drones avanza constantemente, y la industria presenta innovaciones en la aerodinámica, motores, materiales constructivos, sistemas de navegación, sistemas de comunicaciones, sensores y otros, pero en este trabajo particular nos centraremos específicamente en aquellos componentes que emplean el *espectro electromagnético y el ciberespacio*. Son los que participan en la guerra electrónica y la ciberguerra.

¿Como funcionan los drones?

Los drones cuentan con un sistema de control de vuelo que les permite realizar los desplazamientos y maniobras necesarias en el aire. Estos movimientos son controlados desde tierra por un operador humano, aunque pueden realizar acciones en forma autónoma.

Además cuentan con un *sistema de comunicaciones* con su base en tierra.

Los planes de vuelo se definen previamente al despegue y los drones suelen seguir estos planes con muy poca flexibilidad. En otros casos, los drones son maniobrados desde la base por un operador humano.

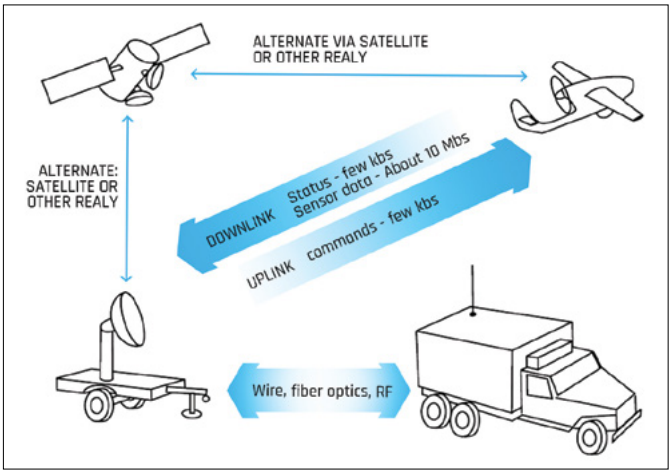
En el dron, existe un sistema de control que contiene *software* para desarrollar las acciones necesarias para el vuelo, mantenimiento de la ruta elegida o navegación, y operación de sensores y sistemas de armas, o de guerra electrónica, y en algunos casos ya cuentan con inteligencia artificial para desarrollar algunas acciones en forma autónoma. Lo que disponga o combinando ambas.

El drone opera en el *espacio aéreo de combate real*, mientras que el sistema de comunicaciones lo hace en el *espectro electromagnético y el software en el ciberespacio.*

Según su misión operacional existen diversos tipos de drones, los mas grandes en general orientados a un empleo estratégico, con gran autonomía y alcance, hasta el nivel táctico inferior dónde encontramos drones pequeños, de limitada autonomía y muy corto alcance.

IMAGEN: "DRONES, LA PRÓXIMA GUERRA" – FIE 2019.

1. **Sistema de Comunicaciones**



Cuentan con un enlace de datos o datalink para dos finalidades básicas:

> UPLINK: permite el comando del UAV y su carga útil.

> DOWNLINK: permite el Control y bajada de información de la carga útil (Telemetría, velocidad, RPM, video, etc) y tiene mayor BW que el anterior

La finalidad principal es mantener las comunicaciones para comandar y controlar la aeronave en vuelo ya que, el piloto se encuentra en tierra y mantiene su responsabilidad sobre el UAV. Estas son funciones básicas que deben cumplirse en todo drone, pero pueden existir otras en función de su magnitud y empleo operacional.

Los componentes básicos de un enlace de datos son:

> ADT, es el terminal de datos de aire (receptor/transmisor, codificadores, compresores de datos, antenas,etc).
> GDT, terminal de datos de tierra (antenas, receptor/transmisor, decodifcadores, modems, etc).

2. Sistema de control

El sistema de control está diseñado para controlar los vehículos en modo automático, semiautomático o manual. Permite el despegue, el vuelo y aterrizaje del drone.

Está compuesto por dispositivos electrónicos, servomecanismos y actuadores sobre los componentes de vuelos y de misión del drone.

Para realizar las funciones de control, el sistema cuenta con *software embebido* en sus componentes.

Por medio del *sistema de comunicaciones* (data link) se conecta con la estación de control en tierra.

3. Sensores

Los sensores son elementos capaces de medir magnitudes del entorno, que servirán tanto para el propio funcionamiento y vuelo del drone, como para cumplir con su misión particular, la detección de amenazas, obtener blancos para sus sistemas de armas o información de observación de blancos o inteligencia, tanto para transmitir a su base de control, como para emplear en los casos que pueda actuar en forma autónoma y decidir acciones de combate.

Pueden ser elementos simples, para detectar alguna magnitud física o complejos, asociados a transductores y elementos de procesamiento de las magnitudes detectadas. Emplean en estos casos software embebido y el espectro electromagnético.

Mediante los sensores el drone percibe el entorno o la realidad del campo de combate. Su calidad y precisión será muy importante.

4. Sistema de armas

Algunos drones cuentan con capacidad ofensiva, y pueden actuar contra determinados blancos, objetivos definidos, sistemas de armas u otros drones.

Esto es muy amplio, dependiendo del tipo y tamaño del drone, pudiendo portar desde misiles (como Hellfire en drones de largo alcance) o munición merodeadora en drones de corto alcance, denominados "kamikase", porque una vez localizado el objetivo se lanza sobre el mismo como proyectil.

También pueden portar equipo para guerra electrónica, como receptores de escucha de emisiones de comunicaciones o de sistemas de armas, e interferidores para actuar ofensivamente sobre los sistemas electrónicos del enemigo.

Pueden en general actuar en forma autónoma o recibir comandos de su piloto en tierra.

Los drones en el campo de combate

De lo visto anteriormente, ya podemos inferir que los drones participan en el campo de combate, por lo menos en tres espacios: el *espacio aéreo o espacio real,* el *espectro electromagnético,* por el intenso uso que hacen por parte de sus sistemas de comunicaciones, de control, de guerra electrónica, de sensores y sistemas de armas, y por último del *ciberespacio*, puesto que tanto los

sistemas del drone señalados anteriormente, como los sistemas de comando y control en tierra emplean software y redes de datos.

Estos sistemas que emplean intensivamente el espectro electromagnético y el ciberespacio, lo hacen porque permiten muchas funcionalidades y ventajas desde su diseño hasta su operación en combate.

Pero también, el uso de estos espacios, abre vulnerabilidades que pueden ser explotadas por el enemigo, que podría tener acceso a esos espacios.

En el espacio aéreo, que no es motivo de este trabajo, se enfrentan con sistemas de defensa aérea convencionales, frente a los cuales presentan ventajas, y con sistemas anti drones mas modernos y adecuados a este tipo de aeronaves.

En el espectro electromagnético y ciberespacio se enfrentan a las contra medidas del enemigo en el dominio de la guerra electrónica y la ciberguerra, y a la vez, ejecutan acciones de guerra electrónica contra sus objetivos.

Guerra electrónica

En este contexto, podemos analizar esto desde el punto de vista ofensivo o defensivo. También desde el punto de vista de la obtención de información, que genera inteligencia que puede emplearse para el ataque o para la defensa, tanto en comunicaciones como en los sistemas de armas.

EE. UU marcó el liderazgo del empleo de drones, luego el mundo siguió ese camino.

En el conflicto de Ucrania de 2014 sus unidades fueron diezmados por la artillería rusa de largo alcance. Los drones rusos proporcionaron datos de ubicación precisos en tiempo real, utilizando sistemas de guerra electrónica SIGINT / ELINT. Al mismo tiempo, Turquía e Israel produjeron grandes avances, que con la experiencia de empleo en Libia y Siria, ahora participaron del conflicto de Nagorno Karabaj.

Aquí se manifiesta toda la experiencia de Turquía e Israel, las nuevas tecnologías y una doctrina de empleo para estos recursos, por parte de Azerbaiyan, mientras que Armenia, por los resultados vistos no pudo aplicar eficazmente contramedidas contra el arsenal de drones, de su enemigo, es decir no pudo emplear el espectro electromagnético a su favor, tanto para detectar, como para anular estas amenazas.

El uso novedoso por Azerbaiyán al principio del conflicto de "drones" biplanos AN-2 soviéticos antiguos y baratos, como plataforma de sistemas de guerra electrónica pudo engañar a los sistemas de defensa aérea armenios, incluidos los complejos TOR y S-300 modernos suministrados por Rusia, no porque sean malos, sino porque están diseñados para otro tipo de blancos, como aviones de combate a altas velocidades, en lugar de aeronaves pequeñas y lentas. Más de 30 sistemas de defensa aérea armenios fueron destruidos por drones turcos TB2 armados con equipos EW (Electronic Warfare) antirradiación y misiles.

En este caso, los drones cuentan con sensores para detectar la radiación generada por los sistemas de defensa aérea y esto sirve para direccionar los misiles para destruir el blanco.

Por otro lado, los denominados drones kamikase o merodeadores Harop, Orbiter o Kargu, de menor tamaño son mas difíciles o imposibles de detectar por los sistemas de defensa aérea convencionales, cuentan con sensores de radiación para atacar a los sistemas de defensa aérea terrestres y con sensores electro – ópticos para detectar diversos blancos como blindados o artillería, y en este caso interviene el operador remoto que identifica en su pantalla el objetivo y decide el ataque, aunque podrían existir ya algunos que operen en forma autónoma.

En este caso, la transmisión del data link entre el drone y el operador remoto podría ser bloqueada, si previamente se hubiera detectado la frecuencia de trabajo. Sin embargo, en el marco

táctico, si no se detectó y anuló el drone antes, es difícil generar una respuesta efectiva por el escaso tiempo disponible después de lanzar el ataque. Sobre todo los drones mas pequeños, que entre el momento que se lanzan hasta que llegan al objetivo a corta distancia transcurre muy poco tiempo para detectarlos y anularlos.

Sin embargo, Armenia contaba con sistemas Repellent de origen ruso. El sistema Repellent está diseñado para la inteligencia de señales de los UAV y la supresión de sus sistemas de control. Este sistema esta especialmente diseñado contra los UAV de pequeño tamaño.

Tal vez podrían haber sido útiles los radares de efecto Doppler, como los empleados para vigilancia terrestre y aeronaves de baja altura, pero requeriría un entrenamiento específico en detectar ese tipo de amenazas antes de operarlos. Además, no están directamente vinculados a un sistema que genere una contramedida contra el drone, pero si puede dar una alerta temprana.

Según declaraciones atribuidas por analistas al primer ministro armenio, Nikol Pashinyan, al menos habría operado un sistema Repellent, que según la misma fuente no funcionó. No sabemos si por las características del equipo mismo, la capacitación de los operadores armenios, o las acertadas tácticas y medidas del Ejército azherí. Sin embargo, la misma fuente cita que elogió otro sistema de fabricación rusa, los sistemas de misiles antiaéreos Osa-AK,que, según Pashinyan, alcanzó muchos objetivos durante la guerra en Nagorno-Karabaj, y durante la escalada de julio en Tavush derribó un avión no tripulado Hermes 900 israelí empleado por Azerbaiyán.

La misma fuente cita la destrucción de un sistema Repellent cerca de la frontera por un drone turco TB-2. En este caso, el sistema Repellent debió estar protegido por otro sistema de armas, puesto que está diseñado para interferir pequeños drones, y no un TB-2.

Se afirma que otro sistema EW ruso, el Krasuskha, desplegado alrededor de la base Gyumri en Armenia, ha derribado al menos 9 drones Bayraktar, además de las municiones israelíes Harop merodeadoras.

Estos datos no fueron confirmados aún por las autoridades de ambos bandos. Si fuera cierto, confirmaríamos que Armenia si contó con contramedidas anti drones, y sabía que su enemigo los poseía, sin embargo, o bien no fueron suficientes, no fueron bien empleados, o simplemente Azerbaiyán estaba mejor preparado y ejecutó las acciones acertadas.

Otra posibilidad puede ser que la capacidad de detectar y derribar drones no fuera suficiente para cubrir un amplio campo de combate y los azeríes pudieron aprovechar espacios y activos sin esta defensa.

Se conoce también que este sistema ha defendido con éxito la base aérea rusa de Hmeymim en Siria.

Este sistema es construido por KRET (Rusia), y es una estación de interferencia multifuncional de banda ancha que fue diseñada principalmente para proteger áreas dentro y en cercanías de las bases militares de Rusia donde su potente transmisor puede bloquear los radares aéreos. Sin embargo, los rusos también han encontrado que Krakuskha es útil como contra medida para drones armados. Sin embargo, la recepción de estos sistemas Krasuskha no está confirmada según algunos analistas.

Apenas dos días antes de que se firmara un armisticio trilateral, el representante del Ministerio de Defensa de Armenia, Artsrun Hovhannisyan, afirmó que la parte armenia había establecido un récord mundial al derrotar a Bayraktars. Las autoridades armenias afirmaron el 20 de octubre de 2020 que se habían derribado alrededor de diez Bayraktars. La cantidad de drones derrivados por Armenia es contradictoria. Oryx , un blog militar que documentó pérdidas de armas en ambos lados basándose en evidencia visual disponible en fuentes abiertas, contó solo dos pérdidas de Bayraktar TB2 durante la guerra. Al mismo tiempo, las autoridades de Armenia

publicó fotografías de aviones no tripulados TB2 caídos en tres ocasiones (20 de octubre , 22 de octubre y 8 de noviembre). Pero no sabemos si todo es real o lo es solo en parte. Si hubo derribos de drones TB2, habrá sido en un primer momento, y luego el ejercito azerí aplico las decisiones y contramedidas correctas y todo cambió.

Para este caso particular, el Bayraktar TB2 es un avión bastante grande con una envergadura de 12 metros, más grande, de hecho, que el de un caza F16, por lo que debería haber sido detectado y derribado sin problemas por la defensa aérea armenia. Sin embargo, estos UAVs siguieron operando sin mayores dificultades, lo que hace suponer que la guerra electrónica del ejercito azerí marcó la diferencia y fué el elemento clave para lograr el dominio del cielo. Supieron dominar el espectro electromagnético. En este punto cabe suponer que la estrella fué el sistema de guerra electrónica KORAL turco, que está diseñado para bloquear canales de comunicaciones inalámbricas y de radar. DefenseWorld.net, una publicación de Internet, argumentó que Turquía tuvo éxito con las defensa aérea siria por su guerra electrónica empleando un sistema KORAL cerca de Idlib, contra los los sistemas de defensa aérea de fabricación rusa. A principios de 2020, UAVs turcos lograron destruir un SA 22 Panzir de fabricación rusa en el norte de Siria y Libia, a pesar del rango letal superior del Panzir.

En ambos casos, la supresión de los sistemas de defensa aérea fue seguida rápidamente por la destrucción intensiva de los blindados en el campo de combate.

Por lo tanto es muy posible que este sistema de guerra electrónica turco haya intervenido con éxito en este conflicto. El simple hecho de que los UAV lograron pasar desapercibidos a corta distancia podría inferir una acción de guerra electrónica que cegó los radares armenios, aunque ninguna de las partes diga nada aun.

Pero no menos impresionante fue la destrucción de al menos dos sistemas de defensa aérea S-300 dentro de Armenia por drones kamikase HAROPs israelíes. En los videos tomados desde los HAROP se pueden ver las antenas de radar de los sistemas de armas aún girando antes de ser impactado, obviamente sin haber detectado la amenaza de los UAVs que se lanzaban sobre ellos. En este caso, la pregunta del por qué no fué detectado es más fácil de responder: el HAROP es una pequeña aeronave que podría caer por debajo del umbral de detección del radar antiguo del sistema S-300, diseñado para aeronaves mas grandes.

Consecuentemente, una vez que las defensas aéreas armenias fueron neutralizadas, entonces los UAVs azeríes fueron a atacar a los blindados, la artillería y los trenes logísticos. Se publicaron videos azeríes con decenas de tanques, piezas de artillería y camiones de suministros que fueron alcanzados y destruidos por los drones.

Pero finalmente, del lado armenio, como se adelantó precedentemente, aparece el sistema ruso KRASUKHA con gran éxito negando el empleo del espectro electromagnético a los drones azeríes, pero ya la guerra estaba a favor de Azerbaiyán. El conjunto de vehículos aéreos no tripulados de Azerbaiyán dejó de ser efectivo frente a este sistema y podría haber cambiado la batalla si se hubiera empleado desde el principio del conflicto, o no si el lado azerí hubiera acertado con las contra contra medidas electrónicas. Por ahora esto es solo una conjetura y la guerra ya está resuelta.

Todos los UAVs dependen de enlaces de datos seguros con sus operadores humanos ubicados en su sector del campo de combate, y siempre siguen siendo vulnerables a interrupción por interferencia electrónica o al engaño.

Ciberguerra

El ciberespacio es el dominio mas abstracto, mas difícil de controlar, tanto en la ofensiva como en la defensa. El conocimiento es el activo mas importante. En los equipos militares el fabricante

se niega a divulgar el código fuente y los algoritmos. Además usualmente se reserva un método de acceso para mantenimiento y actualizaciones. Cabe destacar que el software embebido, así como los sistemas de información en general, permiten mejorar funcionalidades y prestaciones, y hasta incorporar nuevas sin necesidad de cambiar el equipo o hardware.

Nunca sabe quien compra el equipo si el proveedor entrega lo mismo que usa su pais o alguna variante diferente, incluso si tiene alguna "puerta trasera" o acceso especial no controlado por el usuario. Existe aún poca información confiable sobre este punto, solo podemos destacar que la lucha en el ciberespacio existe y tiene diversos fines, algunos con objetivos militares específicos como el engaño emitiendo señales de GPS falsas captadas y denunciadas por buques que navegan en el Mar Negro y Mar Meridional de China, atribuidas a hackers rusos y chinos respectivamente, hasta la captura de un dron israelí por parte de fuerzas iraníes que lograron tomar y engañar a su sistema de navegación.

En esta guerra, no encontramos información aún de este tipo de acciones de ciberguerra que afecten a sistemas de armas, pero si son claras las acciones en las redes sociales, seguramente promovidas por el ejército azerí tendientes a socavar la moral de las fuerzas armadas y el pueblo armenio.

Estas acciones consistieron en difundir por redes sociales videos e imágenes del poder militar azerí, basado en los drones, destruyendo activos militares armenios, y mostrando que no tenían ninguna posibilidad de defensa frente a este tipo de ataques. Esto sin duda afecto la moral y la voluntad de lucha de los armenios, teniendo en cuenta que el acceso a redes sociales es personal, y que una eventual censura acarrea también otros costos, además de la posibilidad concreta de implementarla.

Sistemas EW que probablemente participaron

I. Sistema Repellent – Rusia

Es un sistema de guerra electrónica contra UAVs de pequeño tamaño. Provee protección de zonas de gran eficacia.

Cuenta con capacidad de supresión radioelectrónica de los canales de control de cualquier UAV.

El sistema Repellent está diseñado para la inteligencia de señales de los UAV y la supresión de sus sistemas de control. El sistema proporciona:

> Detección y radiogoniometría de los sistemas de control y transmisión de datos de los UAV, suponemos incluye la detección de la estación de control en tierra.
> Seguimiento de los parámetros de la señal de los UAV.
> Procesamiento estadístico de parámetros de señales, formulación de atributos de clasificación, soporte de bases de datos de inteligencia de señales y clasificación de señales.
> Supresión electrónica de los canales de control y transmisión de datos de los UAV y de las estaciones de control en tierra.
> Bloqueo del receptor de navegación por satélite de los UAV.

Puede estar configurado tanto en versión móvil como estacionaria.

Provee Inteligencia de señales y ancho de banda de frecuencia de supresión electrónica entre los 200 a los 6000 MHz.

Cuenta con un alcance de inteligencia de señales de al menos 30 km y puede interferir para lograr la supresión electrónica en esa distancia hasta los 30 km, suficiente en el marco táctico.

II.Sistema Krasukha - Rusia

El Krasukha está diseñado para bloquear AWACS (Airborne Warning and Control System) a distancias de hasta 250 kilómetros (160 millas). El Krasukha también es capaz de bloquear otros radares aerotransportados, como misiles guiados por radar. A los misiles, una vez bloqueados, se les proporciona un objetivo falso alejado del original para garantizar que los misiles ya no sean una amenaza. El Krasukha protege objetivos La estación de interferencia multifuncional de banda ancha Krasukha está montada en un chasis de cuatro ejes BAZ- 6910-022. Al igual que el Krasukha sirve como contra medida para contrarrestar el AWACS y otros sistemas de radar aerotransportados.

El Krasukha-4 también tiene el alcance eficaz para interrumpir los satélites de órbita terrestre baja (LEO) y puede causar daños permanentes a los dispositivos montados en ellos.

III.DZUDOIST (MKTK-1A) - Rusia

Es un sistema automatizado móvil para monitoreo de radiofrecuencia protección de la información y evaluación del entorno electromagnético basado en equipos especiales. Esta en el dominio de la Guerra Electrónica de Comunicaciones y sistemas de comando y control.

El sistema Dzudoist proporciona la solución de una de las tareas principales de EW: la protección radioelectrónica de las comunicaciones y los enlaces de control contra el reconocimiento técnico del enemigo.

El sistema Dzudoist está diseñado para la detección y posicionamiento de fuentes de señales de radio, bloqueo de canales técnicos y laterales de fuga de datos, y también para verificar la compatibilidad con los requisitos de contramedidas contra el reconocimiento técnico del enemigo.

El sistema se puede utilizar para un monitoreo técnico integral en instalaciones estatales y militares con la misión de evitar la filtración de información clasificada.

Cuando se despliega en el campo de combate, el Dzudoist controla la seguridad de las comunicaciones y la protección de los modos de operación establecidos de los equipos de radio.

El sistema está equipado con diferentes medios de monitorización de canales radio, receptores de banda ancha y analizadores de espectro.

El sistema incorpora tres estaciones de trabajo automatizadas: para monitoreo de radio, análisis técnico y control especial.

El software dedicado instalado en las estaciones de trabajo procesa rápidamente la información que genera resultados de control y datos de análisis del espectro electromagnético en un mapa digital del terreno y también identifica las fuentes de señales.

El espectro de operación es muy amplio, va desde 0,1 a los 18,000 Mhz, e incluye la detección de pulsos electromagnéticos y señales acústicas.

Para su movilidad en el campo de combate está montado en un camión Kamaz 4350.

IV. Elbit Hermes 900 – Israel

Azerbaiyán mencionó por primera vez la adquisición del Hermes 900 en agosto de 2017, informando que se habían comprado hasta 15 unidades. Desde el punto de vista de la Guerra Electrónica, tiene capacidad para portar sistemas EW, puesto que posee una capacidad de 350 kgr. de carga útil. No se ha encontrado que tipo de sistemas EW portaron en este conflicto, pero sin duda fueron efectivos.

V. UAV Bayraktar TB2 – Turquía

Empleado por Azerbaiyán, fabricado en Turquía por Kale-Baykar. Posee una carga útil de 150 kgr y un alcance de 150 km. Porta cámara IR y EO, designador láser y telémetro láser (LRF). Como arsenal ofensivo, puede llevar hasta cuatro misiles Roketsan MAM-L / MAM-C.

VI. Sistema de guerra electrónica de radar terrestre Koral – Turquía

El sistema de guerra electrónica de radar terrestre KORAL está diseñado y fabricado por la compañía de defensa turca Aselsan. El sistema KORAL está compuesto por dos camiones militares 8x8, cada uno con un elemento del sistema. Uno es el soporte electrónico de radar (ES System) y un sistema de ataque electrónico de radar múltiple (EA) para cubrir el espectro completo.

El sistema KORAL respalda las operaciones de Supresión de Defensa Aérea Enemiga(SEAD) mediante la construcción del dominio de la información y proporcionando un tiempo de respuesta rápido en el campo de batalla. KORAL se compone de soporte MAE (Medidas de Apoyo Electrónico) electrónico y sistema de ataque electrónico CME (Contra Medidas Electrónicas) cada uno montado en un camión táctico ocho por ocho.

El Sistema KORAL es operado por dos operadores dentro de la Unidad de Control de Operaciones (OCU), un Operador de Soporte Electrónico para las funciones de detección, análisis y DF (radiolocalización) y, un Operador EA para las funciones de interferencia, engaño y asignación

de fuentes. Además, el supervisor dentro de la OCU maneja la coordinación operativa y la comunicación con los otros sistemas y comandos de KORAL.

Con un alcance efectivo de más de noventa millas (unos 150 kilómetros), se informa que KORAL podría bloquear y engañar cualquier sistema de radar terrestre, marítimo y aéreo. La dirección del haz rápido se genera a través del sistema de antenas de matriz en fase con una alta salida de potencia y múltiples amplificadores de estado sólido. El sistema cubre una amplia cobertura espacial y de frecuencia con una alta precisión de medición de parámetros.

Conclusiones

En este corto conflicto vimos un rápido triunfo de Azerbaiyán sobre Armenia, en el que los vehículos aéreos no tripulados de Azerbaiyán destruyeron la formidable variedad de defensas aéreas terrestres de Armenia, y posteriormente diezmaron sistemáticamente el material de sus fuerzas terrestres, incluidos tanques, piezas de artillería y camiones logísticos. Este ataque obligó a Armenia a aceptar el alto el fuego impuesto por Rusia.

Parece, según los analistas, que la clave de la espectacular victoria azerí fué el empleo de los vehículos aéreos no tripulados de Azerbaiyán que infringieron severos daños a su enemigo.

Sin embargo, ese es el resultado tangible en el campo de combate y el espacio aéreo.

Luego de los expuesto en este documento, también podemos concluir que Azerbaiyán ganó el *espectro electromagnético* y el *ciberespacio*. Dos espacios intangibles, no delimitados en la cartografía militar, pero que posibilitaron que los drones puedan operar en el espacio real.

Este conflicto, y en particular la guerra electrónica y la ciberguerra está siendo observado por analistas militares de las principales potencias del mundo, que ya pueden observar sus propias debilidades y proyectar, al menos hipotéticamente, como hubiera funcionado su propio poder de combate enfrentado contra estas tecnologías.

Por último, en estos espacios, si bien es necesario el equipamiento adecuado, mucho mas importante es el *conocimiento*. A una acción ofensiva se le opone una contra contra medida, y cualquier bando puede hacer que el sistema del enemigo se comporte como obsoleto, si actúa correctamente. Si bien en estas operaciones existen también procedimientos estandarizados, mucho mas importante es la adaptación proactiva de las respuestas a las acciones ofensivas, que solo logra el personal con sólida formación tecnológica y científica.

No solo será importante estar preparado para la guerra, sino también, una vez en ella poder adaptarse rápidamente a los desafíos que ésta impone.

Fuentes

> Franz-Stefan Gady , Alexander Stronell “Lo que reveló el conflicto de Nagorno-Karabaj sobre las futuras guerras” - Word Politic Review.}
> Ministerio de Defensa de Estononia.
> Extractos de Bloomberg, opinión.
> DefenseWorld.net
> Aselmam - Electronic Warfare Systems.
> Sociedad anónima Rosoboronexport.
> Elbit Systems.
> Noticias de Israel.

(*) **Rafael Mario Olivieri** es Coronel del Ejército Argentino en situación de retiro, promoción 116, Arma de Comunicaciones, Ingeniero Militar especialidad Informática, Especialista en Redes de Datos, Analista del Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la FIE. Se desempeñó en diferentes proyectos de desarrollo de software y comunicaciones en el Ejército Argentino, profesor de Sistemas Operativos, Comunicaciones, Redes y Teoría de Control; ha realizado publicaciones sobre su especialidad.