Por otra parte, la mayoría de los detenidos por yihadismo entre 2013 y 2016 usaron las redes sociales o foros en sus procesos de radicalización. No obstante, las plataformas más influyentes en este campo son actualmente los foros privados y las aplicaciones de mensajería instantánea, ya que permiten una comunicación más segura y dificultan las actividades de monitorización de los servicios de seguridad.

Los perfiles más comunes entre los yihadistas detenidos en España son inmigrantes marroquíes de segunda o tercera generación que no se sienten identificados con ninguna patria y son vulnerables a la radicalización. En este contexto, Internet juega un papel esencial en estos buscadores de identidad, ya que contribuye a proporcionar un sentido de pertenencia a la *ummah* virtual.

Otro factor que afecta únicamente a España es el hecho de que la narrativa yihadista contiene un elemento no común en otros países. Se trata de la recuperación de Al-Ándalus como parte de un futuro califato. Los expertos mostraron que la presencia de este discurso es extensa en la propaganda yihadista en España. Así, este país no es un objetivo yihadista solo por su participación en campañas militares en países de mayoría musulmana como ocurre con otros Estados occidentales.

Por último, se analizó la prevención de la radicalización online en España. Se concluye que una estrategia de contranarrativa contra el discurso yihadista en Internet es el enfoque más acertado para prevenir este fenómeno a largo plazo. El Plan Estratégico Nacional contra la radicalización violenta —implementado en 2015— incluye este elemento como parte del programa. Sin embargo, ha recibido críticas por no ser efectivo. En este sentido, se alega que es demasiado pronto para evaluar su efectividad, ya que es una estrategia a largo plazo y se puso en marcha hace solo unos pocos años. También contempla el tratamiento de los individuos radicalizados y se concluye que un objetivo de desradicalización no es viable. De esta forma, el procedimiento del plan se centra en desenganchar a los extremistas de la violencia, independientemente de si sus creencias radicales siguen estando presentes en sus mentes o no.

Víctor Torralba Rodríguez
Graduado en el Máster de Seguridad Nacional
King's College London

ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

11/2019 5 de febrero de 2019

Fernando Manrique Montojo *

Panorama de la guerra electrónica en Rusia

Panorama de la guerra electrónica en Rusia

Resumen:

Si existe una faceta de la reforma militar rusa que está atrayendo la atención de los expertos, esa es la relativa a la guerra electrónica. Esta disciplina, por su alto grado de especificidad así como por la escasez de información disponible, es una de las grandes desconocidas de la guerra moderna incluso para los profesionales. Es por ello que un documento de estas características se hace necesario para todos los interesados en la evolución del nuevo Ejército ruso.

Palabras clave:

Guerra electrónica, Fuerzas Armadas, Rusia, tecnología, programas de armamento.

Overview of Electronic Warfare in Russia

Abstract:

If there is one facet of Russian military reform that is attracting the attention of experts, it is electronic warfare. This discipline, due to its high degree of specificity as well as the scarcity of available information, is one of the great unknown of modern warfare even for professionals. That is why such a document becomes necessary for all those interested in the evolution of the new Russian army.

Keywords:

Electronic warfare, Armed Forces, Russian federation, technology, weapons programmes.

En los últimos años se ha escrito mucho acerca de la innovación militar. Concretamente, uno de los autores más reconocidos, Stephen P. Rosen, consideraba que una de las mayores características de las grandes innovaciones militares es la aparición de una nueva especialidad y de nuevos tipos de unidades[1]. Las reformas que ha atravesado la guerra electrónica (*Electronic Warfare*, EW) en Rusia han dado lugar precisamente a la creación de una nueva especialidad, dotada de equipamiento, doctrina y orgánica específicas, que aspira a seguir creciendo hasta convertirse en un elemento central de las Fuerzas Armadas de la Federación Rusa (RFAF). En este documento analizaremos desde distintos puntos de vista cómo se han llevado a cabo las reformas que han dado lugar a esta especialidad.

Desarrollo histórico

La guerra electrónica, pese a su aparente modernidad, es una especialidad con una considerable antigüedad. El Ejército ruso remonta su creación hasta la guerra ruso-japonesa, concretamente al 15 de abril de 1904, cuando unidades rusas fueron capaces de impedir la corrección del fuego naval japonés contra Port Arthur, al interferir sus comunicaciones por radio. Actualmente, las tropas de EW celebran su aniversario en esa fecha, aunque probablemente sería más realista buscar sus orígenes en la Segunda Guerra Mundial, ya que estas unidades jugaron un papel importante en algunas batallas. Su desarrollo continuó durante la época soviética, especialmente a partir de 1956, año en que la URSS creó los primeros batallones de interferencias, pero también en las décadas siguientes, pues siguió madurando doctrinal y organizativamente, expandiendo poco a poco sus capacidades hasta llegar a los años 80. En esta década, el general Orgakov[2] desarrolló el concepto de «revolución tecnológica militar» (RTM), según el cual, la superioridad tecnológica era el factor determinante de la eficacia de un ejército. Para sostener su punto de vista, ponía como ejemplo la mejora que la naciente informática podía proporcionar a las municiones, lo que posteriormente quedó demostrado con la aparición de las municiones de precisión durante la primera guerra del Golfo (1991-92). El cese de este general y la caída de la URSS impidieron que sus ideas se llevaran a la práctica pero estas no cayeron en saco roto ya que no fueron pocos los estrategas rusos que supieron reconocer el potencial de sus teorías.

[1] ROSEN, Stephen P. *Winning the Next War. Innovation and the Modern Military*. 1991, pp. 20-21.
[2] Nikolai Orgakov, jefe del Estado Mayor Soviético entre 1977 y 1984.

La turbulenta década de los noventa no permitió avances significativos en relación con la EW, si bien es cierto que durante la segunda guerra de Chechenia (1999-2009) elementos de esta especialidad se integraron en las unidades de reconocimiento con buenos resultados[3]. Tanto es así, que en 2002, casi al mismo tiempo que se abandonaba el tratado ABM[4], un Vladimir Putin recién llegado a la presidencia rusa firma una directiva a largo plazo para el desarrollo de la EW en las RFAF[5], fruto del cual se produjo el rápido desarrollo de esta especialidad. En 2009, tras la guerra de Georgia y en plena efervescencia derivada de la aplicación de las reformas de Serdyukov, se crean las tropas de EW, si bien el único efecto a corto plazo de esta medida, fue la creación del Cuartel General de EW dentro del Estado Mayor General[6]. Este centro de mando será fundamental para dirigir y coordinar las acciones entre los distintos ejércitos así como para racionalizar la adquisición y modernización de los materiales. No en vano poco después se firma el programa estatal de armamento (GPV) 2011-2020, que retoma muchos proyectos soviéticos abandonados pero ahora con un nivel tecnológico superior. Un año después, se renueva la estrategia de desarrollo de la EW con el horizonte puesto en 2020.

En los años siguientes, como parte de las reformas *New Look*, se crearon compañías de EW en todas las brigadas del Ejército. Casi al mismo tiempo, se diseñó la orgánica de las brigadas independientes de EW; las cuales se beneficiaron de un elevado ritmo de entrega de nuevos equipos. Estudiaremos sus orgánicas más adelante. En 2013, las nuevas unidades pasan a integrarse en una nueva especialidad de EW dentro del Ejército de Tierra[7] y un año después, el VDV[8] hizo lo propio, creándose además ocho compañías, una por cada gran unidad del cuerpo. Sin querer profundizar en esta cuestión cabe decir que el resto de cuerpos de las RFAF, es decir la Fuerza Estratégica de Misiles (RVSN), la Fuerza Aeroespacial (VKS) y la Armada rediseñaron también durante este periodo la organización de su EW, por lo que podemos decir que actualmente las tropas de EW tienen un verdadero carácter conjunto.

[3] MC DERMOTT. «Russia's Electronic Warfare Capabilities to 2025». *ICDS*. 2017, p. 13.
[4] Anti-Ballistic Missile Treaty.
[5] KJELLÉN, Jonas. «Russian Electronic Warfare». FOI-R--4625—SE. Suecia: 2018, p. 63.
[6] KJELLÉN, obra citada, p. 29.
[7] En el Ejército ruso existen armas de combate y especialidades de apoyo al combate con un prestigio menor.
[8] El VDV es el acrónimo ampliamente utilizado para referirse a las Fuerzas Aerotrasportadas rusas, que juegan un rol similar para la Federación, al del Cuerpo de Marines en los EE.UU.

Cambios doctrinales

Una manera sencilla de aproximarnos a la evolución doctrinal de la EW es a través de la evolución de las distintas definiciones. Así en los 50, era conocida como «contramedidas de radio», dando a entender que se limitaba a impedir las comunicaciones del adversario. Ya en los 60, se empieza a hablar de combatir el equipamiento radio electrónico enemigo, cambio que vino motivado por la mayor importancia de los equipos radar. Se aprecia que en esa época solo se contemplaban acciones ofensivas (*electronic countermeasures* o ECM en terminología OTAN). En la definición que da la *Enciclopedia Militar soviética* de 1984, ya se diferencia entre acciones ofensivas y defensivas destinadas a proteger las comunicaciones propias (se corresponden con las EPM *electronic protective measures*). No se hace referencia explícita a las medidas de apoyo electrónico (ESM, *electronic support measures*) como detectar, identificar y localizar el origen de las emisiones, señal de que en aquellos momentos no se les daba una importancia especial.

En 1990, el *Diccionario Naval* introduce una nueva definición en la que se habla de actuar sobre los «equipos y sistemas radioelectrónicos». Este cambio da a entender que se amplía el abanico de posibles blancos de la guerra electrónica. El Ministerio de Defensa acabó por hacer suya esta definición con el añadido de incluir una mención a las ESM, bien a un aumento en la importancia de estas medidas o bien una emulación de la doctrina occidental y así figura actualmente en la *Enciclopedia Militar rusa*.

Otra definición digna de mención procede de la Academia del Aire. En ella se distinguen cuatro tipos de acciones de EW, algunas sin equivalente occidental y que indicamos a continuación:

- Ataque electrónico: similar al mismo concepto en la OTAN pero con un carácter más amplio ya que contempla la destrucción física de los equipos, ya sea mediante ataques convencionales o mediante técnicas electrónicas, bien con armas de energía dirigida o de impulso electromagnético, bien mediante acciones cibernéticas. Además contempla la simulación electrónica, es decir la réplica señales electrónicas de determinados equipos a fin de engañar al reconocimiento enemigo.
- Protección electrónica: contempla la protección frente a las ECM y además la compatibilidad de los equipos propios con la EW.
- Medidas radioelectrónicas de apoyo a la obtención de información: principalmente orientadas a la obtención de información del espectro electromagnético.
- Contramedidas frente al reconocimiento técnico: un concepto sin equivalente en la OTAN, cuyo origen estaría en las unidades de control técnico integral (*Kompleksnyi tekhnicheskii control*, KTK por sus siglas en ruso) que operan en las Fuerzas Estratégicas y cuya función es detectar e impedir cualquier emisión involuntaria que pueda revelar la posición propia[9].

Otro aspecto interesante es la relación de la «guerra electrónica» con la «guerra de la información», ya que en la doctrina rusa, esta última engloba tanto la faceta tecnológica (guerra electrónica y cibernética) como la psicológica, como también se puede apreciar en la *Enciclopedia Militar*[10].

Terminaremos esta sección, hablando de otra particularidad de la EW rusa: los distintos tipos de unidades en función del medio en el que actúen. Esta categorización se deriva de que en cada zona de la atmósfera se utilizan distintas bandas del espectro y por tanto cambian los equipos a utilizar, por lo que las unidades organizadas para actuar en cada uno de estos dominios son completamente distintas. Así las unidades de EW se clasifican en cinco categorías que nombraremos por sus siglas en ruso, ya que es la terminología utilizada en las publicaciones que estudian esta materia:

- REB[11]-N: actúan sobre blancos en la superficie, ya sean terrestres o navales.

[9] Es probable que la Fuerza Aeroespacial haya adoptado este concepto con vistas a sus radares y unidades de Defensa Aérea, completándolo después con otras acciones propias (como el cegamiento de aviones AWACS, la preparación de señuelos…) hasta dar lugar a esa cuarta categoría. No es propiamente algo nuevo, pero el hecho de que se les considere un tipo de acción diferente indica una importancia creciente.
[10] De la *Enciclopedia Militar rusa* (Encyclopedia.mil.ru).
[11] *Radioelektronnaia borba.*

- REB-S: actúan sobre blancos aéreos (ej.: aviones y municiones guiadas).
- REB-K: actúan sobre blancos en el espacio (principalmente satélites).
- REB-Atd: unidades antiterroristas.
- KTK: unidades de control técnico integral.

Rearme y desarrollo de nuevos equipos

En una especialidad tan técnica como la de EW, el equipamiento reviste una gran importancia. Además, conseguir dotar de equipos modernos a las unidades es una tarea que muchas veces excede el nivel militar. Es por ello que la modernización y adquisición de nuevos equipos de EW debe estudiarse en el marco de la política rusa de rearme que incluye los programas estatales de armamento (GPV) y la coordinación de las RFAF con la industria de defensa a través de la «Comisión Militar-Industrial» (CMI). Los primeros son documentos a diez años vista que establecen el tipo y la cantidad de los equipos a adquirir, así como la fecha de las entregas. Mientras que esta última es la encargada de coordinar las necesidades de las RFAF en materia de I+D, con los programas y capacidades industriales mediante un sistema que podríamos traducir como: «Sistema Prospectivo para la Investigación y el Desarrollo Militar», gracias al cual se identifican las tecnologías claves para la defensa y se establecen las áreas de inversión en I+D.

No cabe duda de que una de esas áreas de inversión es la guerra electrónica y así lo confirma el gran número de equipos modernos que las tropas de EW recibieron durante el GPV 2010-2020 y los que recibirán en el marco del GPV 2018-2027. Los frutos de esta política estatal son cada día más evidentes. El general Lastochkin, jefe de las tropas de EW, se muestra convencido de que no solo se alcanzará un 70 % de equipamiento moderno en 2020 como estaba previsto, sino que se llegará al 85 %[12], mientras que la mayoría de las especialidades rondarán el 60%[13]. En todo caso, hay que matizar que en ese porcentaje se incluyen no solo los equipos de nueva adquisición sino también los modernizados. El que la mayor parte del equipamiento de EW soviético se mantuviera almacenado, es una de las claves que nos permite entender este rápido desarrollo. La otra es que la industria de defensa siguió desarrollando nuevos productos con vistas a la exportación. Por eso cuando el Gobierno decidió rearmarse encontró una base sólida

[12] «How Good Is Russian Electronic Warfare? (Part I)». https://russiandefpolicy.blog/tag/15th-independent-ew-brigade/. Acceso: 09ENE19.
[13] CONNOLLY, Richard & BOULÈGUE, Mathieu. «Russia's New State Armament Programme Implications for the Russian Armed Forces and Military Capabilities to 2027». *Chaphan House*. 2018.

para sus proyectos. Además, muchas de las investigaciones y proyectos soviéticos no llegaron a perderse sino que se mantuvieron congelados en los diversos centros de investigación, hasta que la mejora de la situación económica permitió revivirlos. El llevar a cabo una revisión de los medios de EW de las RFAF es algo que supera ampliamente los objetivos de este trabajo, sin embargo es necesario describir, al menos ligeramente, los medios con los que cuentan estas unidades ya que serán ellos los que condicionen sus capacidades tácticas; lo cual haremos en el siguiente punto.

Las nuevas unidades

El nacimiento de la especialidad de EW conllevó la creación de nuevas unidades. Hasta 2008, los medios de EW eran operados por secciones específicas de las tropas de reconocimiento. Al crearse la nueva arma, estas secciones se agruparon en una compañía independiente que depende directamente del cuartel general de la brigada.

La orgánica de estas compañías se conoce con bastante profundidad. Con unos cien hombres, se organizan en seis secciones diferentes, lo que a priori pudiera parecer demasiado. En realidad, se explica por las características del Ejército ruso, ya que al no haber suboficiales profesionales, el porcentaje de oficiales es mayor aunque manden unidades de entidad pelotón. Tres de estas secciones están dedicadas a interferir las comunicaciones enemigas, dos de ellas se ocupan de las comunicaciones terrestres en VHF y HF, mientras que la tercera interfiere las comunicaciones aire-tierra en VHF y UHF. La acción de estas secciones es coordinada por la sección de mando de la compañía que cuenta con vehículos de mando y control y con una escuadra de mantenimiento y apoyo técnico. Estas cuatro unidades operan distintos vehículos del complejo Borisoglebsk-2, sistema de EW compuesto por hasta ocho estaciones que trabajan en las bandas de VHF, HF y UHF (la mayoría modernizaciones de equipos soviéticos), coordinados por una estación automatizada de mando y control. El Borisoglebsk-2 es pues la columna vertebral de estas compañías; la pieza clave que permite tanto interferir las comunicaciones enemigas como hacer labores de inteligencia y adquisición de objetivos, al permitir triangular la posición de las emisoras enemigas.

Las misiones respectivas de las otras dos secciones son: actuar sobre las municiones enemigas y enfrentar la amenaza IED[14]. La sección contra-municiones cuenta con medios muy diversos. El Rtut-BM es una estación montada sobre un blindado MT-LB

[14] *Improvised explosive device*, artefactos explosivos improvisados.

cuya función es interferir las espoletas de proximidad de los proyectiles de artillería, de manera que estas detonen antes de llegar al objetivo. Es por tanto un sistema de protección contra artillería y su función táctica es proteger objetivos de alto valor, si bien solo es útil frente a unas espoletas muy concretas. Por su parte la estación Zhitel R-330Zh puede interferir comunicaciones satélite, GPS y GSM. Su principal función es impedir el guiado de las municiones de precisión, distorsionando la señal GPS, pero también han sido utilizados para interferir la señal de guiado de UAV. Su amplio margen de frecuencias y su elevado alcance (15 km para blancos terrestres y hasta 200 km para blancos aéreos) lo convierten en el equipo más potente con el que cuentan estas compañías. También está en dotación en las Brigadas Independientes de EW.

La última sección, que podríamos llamar C-IED, opera quince equipos Lorandit, que son inhibidores portátiles adaptables a vehículos e instalaciones, orientados contra artefactos explosivos terrestres ya sean improvisados (IED) o minas terrestres. Es probable que sea esta sección la que opere el vehículo Infauna, montado sobre BTR. Este sistema no solo tiene capacidad de inhibir este tipo de frecuencias sino que también inhibe la banda de VHF e incluye una serie de detectores ópticos para detectar el disparo de misiles y automáticamente desplegar una cortina de humo.

No hay mucha información acerca de la orgánica de las compañías de EW del VDV, pero podemos suponer que tendrán una organización similar a las del Ejército que acabamos de describir, pero con estaciones montadas sobre vehículos más ligeros que sean fácilmente aerotransportados. Así por ejemplo se sabe que operan el Infauna y el conjunto Borisoglevsk pero sobre camiones[15].

En cuanto a las brigadas independientes de EW la información disponible en fuentes abiertas es mucho menor. A diferencia de la mayor parte de las brigadas de apoyo no actúan en beneficio de los ejércitos de armas combinadas (CAA) sino de los distritos militares (MD), que equivalen a mandos conjuntos. Estas cinco brigadas (una por MD salvo en el MD-Norte y una quinta de reserva) cuentan con unos 1.200 hombres[16] que se organizan en cuatro batallones y una compañía[17], con misiones específicas. Los batallones están orientados a actuar en un medio concreto, de manera que hay

[15] OPEN BRIEFING. «Nobody, but us! Recent developments in Russia's airborne forces (VDV)». 2016, p. 5.
[16] BREAKINGDEFENSE. «Electronic Warfare Trumps Cyber For Deterring Russia». 2018. https://breakingdefense.com/2018/02/electronic-warfare-trumps-cyber-for-deterring-russia/. Acceso: 08ENE19.
[17] MC DERNOTT, obra citada, p. 6.

batallones REB-N, REB-S y REB-K en función de que actúen sobre las comunicaciones terrestres, aéreas o satelitales respectivamente, operando cada compañía medios distintos. El cometido anti-terrorista (REB-Atd) lo desempeña una compañía independiente. Además parece ser que en los últimos años se están empezando a crear compañías específicas para enfrentar a los UAV.

Los equipos principales de los batallones REB-N son el ya explicado Borisoglevsk-2, el Leer-3 y el Murmansk-BM. El Leer-3 es una estación que controla tres drones Orlan que portan equipos de EW de manera que se pueden situar hasta cien kilómetros en el interior del despliegue enemigo. De momento se sabe que han sido utilizados en Siria para duplicar la red de telefonía móvil y así monitorizar las comunicaciones de los rebeldes[18]. Por su parte el Murmansk-BM es un conjunto compuesto por siete camiones, cuatro porta-antenas y tres de mando y control. No es un sistema de acompañamiento, ya que requiere de 72 horas para entrar en posición, por lo que parece formar parte de la EW estratégica, siendo su función interferir la red HFGCS[19]. Se le supone un alcance de más de 3.000 km[20].

En el batallón REB-S prestan servicio equipos como el Krasukha-2O, el Moskva-1 y el ya mencionado Zhitel. El Krasukha-2O es una evolución de los equipos soviéticos anteriores y fue diseñado durante los años 90 con el objetivo de cegar los aviones de alerta temprana tipo AWACS a distancias de 150 km[21]. Por su parte, el Moskva-1 se define como un radar pasivo (es decir que recibe las emisiones de cualquier aparato radiante) de manera que es capaz de triangular sus posiciones hasta a 400 km[22]. Ambos equipos trabajan en coordinación con el Krasukha-4S, que probablemente se encuadre en el batallón REB-K. Este equipo es capaz de interferir los satélites de órbita baja y los radares de las plataformas aéreas. Estos son solo algunos de los equipos ya en servicio, pero en los próximos años comenzarán a desplegarse otros aún más potentes. Uno de los más interesantes es el sistema de mando y control de nivel brigada, conocido como Bylina. Su función será integrar los equipos de mando de batallón y compañía, utilizando inteligencia artificial para seleccionar los blancos y proponer acciones a los usuarios. Las entregas comenzaron en 2018 y deberían finalizar antes de 2025.

[18] DURA, Maksymilian. «Electronic warfare: Russian response to the NATO's advantage? [Analysis]». *Defence24*. 2017.
[19] High Frequency Global Communication System.
[20] KJELLÉN, obra citada, p. 50.
[21] TASS. «Russia's cutting-edge weaponry capable of 'blinding' enemy's army». 2017. http://tass.com/defense/942027. Acceso: 17ENE19.
[22] DURA, Maksymilian, obra citada. 2017, p. 6.

Viendo la panoplia armamentística de estas brigadas podemos deducir que mientras los batallones REB-N apoyarán a las unidades de maniobra de los CAA, los REB-S y REB-K están planteados para colaborar con las brigadas de defensa aérea; de hecho en las unidades de DAA de la Fuerza Aeroespacial cuentan con batallones de EW idénticos a los REB-S. Esto puede confirmarse por el uso que de estos equipos se está haciendo en Siria y Ucrania. En Siria, junto a grupos de S-400 y S-300 PMU, se desplegaron varios Krasukha-4S y Moksva-1[23] que son un quebradero de cabeza para las fuerzas estadounidenses[24] y probablemente hayan tenido mucho que ver en el escaso efecto de los ataques aéreos del 07ABR17 y 14ABR18, pues pese a que ambas potencias dan versiones completamente distintas de lo sucedido, como mínimo está quedando claro que la eficacia se va reduciendo al necesitarse cada vez más medios para lograr los mismos o menores efectos. En el Dombass, el uso de la EW ha sido muy diferente, centrándose en la maniobra terrestre, lo que ha permitido desarrollar tácticas a bajo nivel. Por ejemplo en las batallas de Ilovaystk y Debaltseve los equipos de EW se desplegaron en anillos concéntricos alrededor de la zona a atacar en función de las frecuencias a interferir, las cuales condicionan el alcance de los equipos[25].

Instrucción y adiestramiento

No podemos terminar sin referirnos al adiestramiento en esta nueva arma, ya que es una de las razones de su éxito. El corazón de su sistema de instrucción es el Centro de Enseñanza de Tambov. Es ahí donde los cerca de diez mil soldados de EW han recibido su curso inicial de cuatro meses de duración y también donde las unidades realizan su adiestramiento básico, habiéndose instruido en los últimos once años a cinco batallones REB-N y unas cuarenta compañías. La formación de los mandos así como la específica de REB-S se imparte en la Academia del Aire en Voronezh, impartiéndose también otros cursos específicos en las otras academias. Sin embargo es aún más interesante el analizar los ejercicios que las tropas de EW están llevando a cabo.

[23] SUOMENARO, Matti and CAFARELLA, Jennifer. «Russia Expands Its Air Defense Network in Syria». *ISW*. 2018.
[24]Reproducimos literalmente las palabras del general Raymond Thomas en el transcurso de una conferencia en abril de 2018: «*Right now in Syria we are operating in the most aggressive EW environment on the planet from our adversaries. They are testing us everyday, knocking our communications down, disabling our EC-130s…»*. SELIGMAN, Lara. «Russian Jamming Poses a Growing Threat to U.S. Troops in Syria». 2018. https://foreignpolicy.com/2018/07/30/russian-jamming-poses-a-growing-threat-to-u-s-troops-in-syria/.
[25] MCDERNOTT, obra citada, p. 26.

En 2017, se hicieron 220 ejercicios específicos de guerra electrónica[26], diez de ellos de nivel brigada, lo que supone dos ejercicios tipo GAMMA por cada brigada, y entre cinco y siete ejercicios tipo ALFA por cada compañía. Algunos de estos ejercicios tienen un carácter estratégico, participando varias brigadas y compañías. Así por ejemplo en el ejercicio Elektron-16 intervinieron más de 30 unidades con 460 equipos de EW[27]. Otros ejercicios se centran en aspectos concretos como la defensa aérea, campo en el que se estima que el empleo de los medios de EW en coordinación con la defensa aérea puede aumentar su eficacia en un 30 %[28] o el enmascaramiento, con la participación de unidades de zapadores y de defensa NBQ, para crear respectivamente falsas posiciones y cortinas de humo. Sin descuidar la guerra de la información, como en el Kavkaz 2016[29]. Sin embargo quizás lo más importante es que en los últimos años todas las unidades han comenzado a adiestrarse para operar con un espectro electromagnético saturado y discutido.

Conclusiones

En las páginas anteriores hemos estudiado las reformas que ha atravesado la guerra electrónica rusa durante los últimos diez años, hasta convertirse en lo que es hoy, para seguidamente analizarlas brevemente desde los puntos de vista doctrinal, de equipamiento y organizativo. En base al trabajo anterior podemos extraer las siguientes conclusiones.

Primeramente, debemos decir que el auge de esta arma en las RFAF no es fruto de una situación pasajera sino el resultado de un serio debate en el seno de las mismas. Consecuencia del mismo es que el Estado Mayor General considere la EW como una «respuesta asimétrica a la superioridad tecnológica de la OTAN»[30], un complemento a sus, ya de por sí importantes, capacidades A2/AD[31] y como un «multiplicador de fuerza»[32], capaz de reducir las funciones de combate de mando y control e inteligencia enemigas mientras incrementa la inteligencia, el apoyo de fuegos y la protección propias. Hay que añadir que estas teorías han sido probadas en situaciones reales y de combate.

[26] KJELLÉN, obra citada, p. 69.
[27] KJELLÉN, obra citada, p. 70.
[28] What you need to know about the russia's air/space defense system concept. https://southfront.org/russia-airspace-defense-system-concept/. Accedido: 13ENE19.
[29] ELFVING, Jörgen. «Russian Information Warfare—Not Just Hackers and Trolls». 2016.
[30] KHUDOLEEV, Viktor. «Troops for combat on airwaves». *Krasnaya Zvezda*. 2014.
[31] MCDERNOTT, obra citada, p. 29.
[32] Ibíd, p. 2.

En la campaña del Dombass se pudo observar una gran variedad de medios de EW que no solo limitaron la capacidad de reacción de las fuerzas ucranianas sino que además sirvieron para levantar objetivos a la poderosa artillería rusa; mientras que en Siria se han podido testar algunos de los medios de EW más modernos del arsenal ruso frente a los medios de la Alianza. En este último escenario, es difícil valorar hasta qué punto la EW ha resultado eficaz, sin embargo es indudable que su presencia se ha hecho notar.

Por tanto el balance de estas reformas, ha resultado claramente positivo, por lo que seguramente se mantendrá el propósito de potenciar esta especialidad. Este fortalecimiento es previsible que se realice de varias formas. Por un lado, mediante la modernización de los equipos, estando previsto renovar como mínimo el 70 % para 2020. Por otro, es probable que la llegada de nuevos equipos se traduzca en la creación de nuevas unidades hasta igualar la estructura de otras armas de apoyo, como las Fuerzas de Defensa NBQ, ya que es significativo que los CAA no cuenten con unidades de EW de apoyo directo. Sin embargo el suministro de estos equipos no se limitará a las unidades específicas sino que seguramente se generalizarán los equipos de auto-defensa dotando de ellos a un número creciente de vehículos y aeronaves. Más dudoso resulta que la Federación pueda mantener el ritmo de innovación tecnológica actual, ya que muchos recientes desarrollos proceden de la época soviética. El que lo logren dependerá mayoritariamente de los éxitos de cara a la exportación.

En resumen, es muy probable que las tropas de EW rusas hayan alcanzado un nivel de desarrollo doctrinal y organizativo[33] sin parangón con ningún otro ejército y que por tanto, su capacidad de negar o cuando menos cuestionar el dominio del espectro electro-magnético a sus oponentes sea real. Los ejércitos de la Alianza no deben ignorar estos hechos y en particular nuestro Ejército, en pleno desarrollo del concepto Brigada 2035, puede obtener valiosas lecciones de la reforma militar rusa.

*Fernando Manrique Montojo**
Capitán de Infantería, Brigada Galicia VII

[33] MITCHELL, Ellen. «Army's electronic-warfare training seen as lagging behind Russian efforts». *Inside Defense.* 2015. https://insidedefense.com/inside-army/armyselectronic-warfare-training-seen-lagging-behind-russianefforts. Acceso: 08ENE19.