CAPÍTULO 8

Análisis de la Función de Combate Guerra Electrónica

"El empleo del espectro electromagnético durante la Operación Militar Especial Rusa"

Mayor Christian Cataldo Soto[1]

Introducción

La Operación Militar Especial ejecutada por las Fuerzas Armadas (FAs) de la Federación Rusa sobre el territorio ucraniano a partir del 24 de febrero de 2022, ha mostrado al mundo el empleo integrado, coordinado y sincronizado de medios acorazados, aéreos y productores de fuego, que han traído a la memoria colectiva, la Bliztkrieg alemana utilizada durante la II Guerra Mundial y la potente ofensiva aliada, aplicada en Irak en el marco de la Operación "Tormenta del Desierto" en el año 1991. Es así, que, en el desarrollo de este conflicto

[1] Mayor del Ejército de Chile, del arma de Telecomunicaciones y especialista en Guerra Electrónica. Licenciado en Ciencias Militares y Oficial de Estado Mayor, Academia de Guerra del Ejército de Chile. Bachiller en Ciencias Sociales, Universidad Diego Portales. Postítulo en Conectividad y redes de datos, Academia Politécnica Militar. Diplomado en Ciencias Sociales, Pontificie Universidad Católica de Chile. Diplomado en Campo de Batalla Futuro, Academia de Guerra del Ejército. Diplomado en Historia Militar y Pensamiento Estratégico, Academia de Guerra del Ejército. Candidato a Magister de Historia Militar y Pensamiento Estratégico de la Academia de Guerra del Ejército de Chile. Actualmente, comandante de la Compañía de Telecomunicaciones N.º 10 "San Marcos" en la 1ra Brigada Acorazada "Coraceros". christian.cataldo@ejercito.cl

armado, que se extiende por más de un año, existe un elemento determinante que en nuestro país ha sido poco difundido. Nos referimos a la Guerra Electrónica (EW), aquella función que busca alcanzar la libertad de acción en el empleo del espectro electromagnético (EEM) y evitar que el adversario lo utilice en beneficio propio, no solo para las comunicaciones, sino también para la obtención de información, empleo de radares, dirección del tiro, uso de vehículos aéreos no tripulados (UAV), sistemas de navegación global satelital (GNSS) y por cualquier otro sistema de armas que utilice el EEM para transmitir y recibir información.

A pesar de que la EW no es un elemento nuevo en el campo de batalla moderno, por el contrario, sus orígenes se remontan en lo terrestre a la I Guerra Mundial, donde, ya en la Batalla de Tannenberg (1914) encontramos antecedentes históricos en relación con la interceptación de las comunicaciones rusas por parte de las tropas alemanas y como esta información proporcionó una ventaja en el proceso de toma de decisiones y en el propio desarrollo de las operaciones de aquel conflicto de gran escala (Valderrama, 1980). Del mismo modo, destacan la importancia y los aportes de la EW en la II Guerra Mundial, conflicto árabe – israelí, la Guerra de Malvinas, la 1ra Guerra del Golfo de 1991, por solo nombrar algunos hechos de armas que han sido estudiados para obtener experiencias del empleo de esta silenciosa, pero precisa arma, que ha permitido romper el ciclo de toma de decisiones del adversario, como también conocer su ubicación y dispositivo, constituyendo un multiplicador de combate, a través de los efectos que logra en el campo

de batalla.

Es por ello, que llaman la atención, los escasos antecedentes y análisis que existen en nuestro país, sobre experiencias del empleo táctico y técnico de las unidades de EW, en especial de las unidades de Operaciones de Guerra Electrónica (EWO) rusas en el marco de la invasión realizada desde febrero de 2022 y que puedan constituir una primera aproximación hacia el conocimiento de cómo son utilizadas estas unidades por parte de las FAs rusas.

Consecuente con lo anterior, el propósito de este capítulo es dar respuesta a ¿Cuáles son las experiencias positivas y negativas del empleo de las unidades de EWO rusas que se pueden obtener del conflicto ruso – ucraniano durante el año 2022?

Para lograr dar respuesta al desafío planteado, en primer lugar, se proporciona una visión general de la Guerra Electrónica en Chile. A continuación se exponen la conceptualización de la EW rusa, la vinculación que existe con los modos de empleo relacionados con la llamada doctrina Gerasimov[2] y la Guerra de la Información, pasando a los antecedentes básicos de las áreas y/o campos, modalidad de empleo y unidades de EWO de las fuerzas terrestres rusas, a través de una revisión documental de diferentes fuentes escritas y abiertas que permitan al lector conocer los antecedentes necesarios para comprender el empleo táctico – operacional y técnico de los medios terrestres rusos.

Seguidamente, se presentan un conjunto de experiencias

[22] En alusión al general Valery Gerasimov, Jefe del Estado Mayor General de la Fuerzas Armadas de Rusia.

positivas y negativas, que, a juicio del autor, ejemplifican el empleo de las unidades de EWO terrestres rusas en el conflicto ruso – ucraniano durante el año 2022 y que permitirán realizar una aproximación en relación con la doctrina y criterios de los comandantes utilizados en los diferentes enfrentamientos y combates de esta campaña militar en desarrollo.

Para finalmente y a través de una visión crítica, concluir en relación sobre el empleo del EEM durante la Operación Militar Especial Rusa en el año en estudio, alejados de la mirada convencional occidental, presentando antecedentes que buscarían desarrollar el pensamiento estratégico en los futuros oficiales de Estado Mayor.

Visión general de la Guerra Electrónica en Chile

Con la finalidad de evitar una visión errónea del lector, se expone de manera sintetizada la organización de la Guerra Electrónica en nuestra doctrina, esto para tener los suficientes antecedentes a la luz, que permitan posteriormente extraer las experiencias del empleo de las EWO en el conflicto en estudio.

En primer lugar, según la actual doctrina institucional, la EW es una acción que se realiza para permitir el empleo del EEM por parte de las propias fuerzas y negar su uso al adversario, que se divide en las siguientes áreas: Inteligencia de Señales (SIGINT), Seguridad de Señales (SIGSEC) y Operaciones de Guerra Electrónica (EWO).

En términos generales, SIGINT es una las áreas de la EW que tiene como propósito la obtención de información. Se emplea en los

niveles estratégico y operacional de la conducción militar, a través de la interceptación de señales que permitan obtener la firma electrónica de los medios empleados por un objetivo de interés. Se divide en Inteligencia de Comunicaciones (COMINT) e Inteligencia Electrónica (ELINT) (Ejército de Chile, 2022).

En ese mismo contexto, la Seguridad de Señales (SIGSEC), corresponde a una actividad permanente que buscar controlar y proteger los sistemas de mando y control propios y las comunicaciones emitidas. A diferencia de la SIGINT, la Seguridad de Señales se realiza en todos los niveles de la conducción con la principal tarea de negar el acceso a la información por parte de fuerzas antagonistas. Esta acción se divide en Seguridad de Comunicaciones (COMSEC) y Seguridad de Comunicaciones (ELSEC).

Por último, las Operaciones de Guerra Electrónica (EWO) que son el centro de este capítulo, son acciones concebidas desde la paz que se realizan en la crisis o EPB con el propósito de degradar los sistemas de información del adversario. Se dividen: en Medidas de Apoyo Electrónica (ESM), que corresponden a aquellas que se centran en la obtención de la información con el propósito de confirmar las acciones del adversario; Contramedidas Electrónicas (ECM), también conocidas como Ataque Electrónico (EA), conciernen a aquellas a través del uso de energía buscan impedir el libre uso del EEM por parte de las fuerzas adversarias en beneficio propio; y las Medidas de Protección Electrónica, que atañen a aquellas acciones, tanto pasivas como activas tendientes a proteger las comunicaciones de los medios de obtención que posee el

adversario (2022).

Los elementos anteriormente presentados, constituyen un elemento basal para poder contar con los elementos necesarios para la extracción de experiencias del empleo de las EWO en el conflicto ruso – ucraniano y que puedan tener valor de uso para nuestra realidad institucional.

La Guerra Electrónica rusa

Para comenzar con una aproximación sobre el empleo del EEM por parte de las fuerzas rusas en Ucrania durante el año 2022, es necesario revisar el concepto de Guerra Electrónica empleado por estas. Para ello, se considera el trabajo realizado por Jonas Kjellén (2018), que presenta que para las FAs rusas:

> La Guerra Electrónica es un conjunto de actividades y acciones coordinadas que abarcan el ataque a objetos radioelectrónicos y de información técnica del adversario, la protección de objetos radioelectrónicos y de información técnica propios, las contramedidas contra el reconocimiento técnico y las medidas de apoyo a la información radioelectrónica" (2018: p.22).

La definición de Kjellén (2018), contine un mayor detalle y posee algunas diferencias con la versión occidental americana que define a la EW como "la acción militar que implica el uso de energía

electromagnética y dirigida para controlar el EEM o atacar al enemigo" (Department of the Army, 2021, p.149). De esta revisión, la principal diferencia se centra en la información, ya que, la concepción rusa hace hincapié en ella, lo que permite inferir que se relacionaría con la función Inteligencia y con las Operaciones de Información (INFOOPS), a diferencia de la versión americana que se concentra en el uso de energía electromagnética y al control del EEM.

Además de lo anterior, es necesario incluir el nexo con la Doctrina Gerasimov, nombre otorgado debido a que fue el actual Jefe de Estado Mayor de las FAs de Rusia, Valery Gerasimov, quién plasmó la nueva estrategia rusa, con la inclusión de modos convencionales y no convencionales como parte del desarrollo de la Crisis y el conflicto armado en sí; que para una campaña militar como la Operación Militar Especial ordenada por el presidente Vladimir Putin, considera: una fase de informaciones; el uso de capacidades simétricas y asimétricas para afectar el poder militar adversario; afectación de la opinión pública; acciones con fuerzas de operaciones especiales y finalmente, el desarrollo del engaño y sorpresa para ocultar las propias intenciones (Masalleras, 2022).

Lo interesante de esta nueva concepción de empleo de los medios, es que no existiría una distinción entre los diferentes niveles de la conducción militar y su aplicación sería durante todas las fases del conflicto, buscando lograr la libertad de acción desde el primer momento, constituyendo un desafío para los países de occidente. A partir de esto es posible identificar que la EW sería el instrumento ideal, ya que

su empleo es transversal a todos los niveles de la conducción militar y en los cinco dominios conocidos.

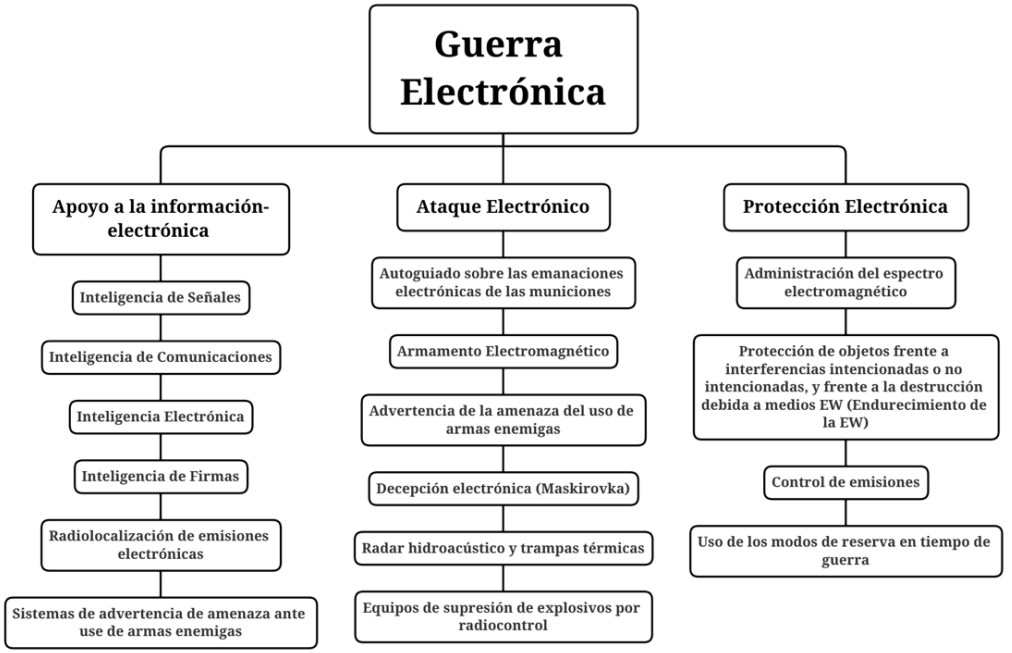
Otro elemento que se debe sumar al presente estudio es la vinculación de la EW rusa con la Guerra por la Información (IW), la cual se caracteriza por su empleo en el amplio espectro del conflicto, buscando afectar la voluntad de las personas, a través de la decepción, el engaño y la búsqueda de la sorpresa, utilizando para ello, las unidades de Guerra Electrónica, tanto como medios de obtención de información, fuegos de destrucción y fuegos no letales, por sus capacidades para lograr el engaño y la decepción electrónica. Lo anterior, se manifiesta como parte de la mencionada Doctrina Gerasimov que vendría a constituir el modelo operacional – táctico para la ejecución de las operaciones en las FAs de la Federación.

Áreas de la Guerra Electrónica rusa

En el estudio "The Russian way of war" (2016), los investigadores Lester Grau y Charles Bartles identificaron tres actividades de la EW rusa: Apoyo a la información electrónica, Ataque electrónico y protección electrónica, las cuales coinciden con la visión occidental, pero la principal diferencia radicaría en los elementos secundarios que consideran cada una de estas actividades, las cuales se presentan en la figura 1.

Figura 1

Actividades de la guerra electrónica rusa



Nota: Elaboración propia, basado en el trabajo de Grau y Bartles "The Russian way of war", 2016.

Como se puede apreciar, a los ya comunes elementos que componen el Apoyo a la información electrónica (en occidente Medidas de apoyo electrónico, ESM), tales como: Inteligencia de señales, Inteligencia de comunicaciones, Inteligencia electrónica, Inteligencia de firmas electrónicas y Radiolocalización, se suma un elemento novedoso, los sistemas de advertencia de amenaza ante uso de armas enemigas. Conforme con ello, es posible inferir que, con la incorporación de esto,

la EW rusa podría monitorear el espectro de manera integral en todas las bandas de frecuencias.

En relación con el Ataque Electrónico (EA), como parte de sus componentes, es posible identificar: Autoguiado sobre las emanaciones electrónicas de las municiones, Armamento electromagnético, Advertencia de la amenaza del uso de armas enemigas, Decepción electrónica (Maskirovka), Radar hidroacústico y trampas térmicas y, Equipos de supresión de explosivos por radiocontrol. Destacándose en esto, la inclusión del empleo de armas que permiten la destrucción física de equipos electrónicos a través del empleo del EEM, el guiado de armamento inteligente y elementos que permiten proporcionar seguridad a las unidades propias en terreno.

Finalmente, la Protección Electrónica (EP) considera la Administración del espectro electromagnético, protección de objetos frente a interferencias intencionadas o no intencionadas, y frente a la destrucción debida a medios EW (Endurecimiento de la EW), Control de emisiones y el uso de los modos de reserva en tiempo de guerra. Con lo anterior, permitiría anticipar cualquier tipo de elemento que ponga en riesgo el empleo del EEM en beneficio propio, logrando la iniciativa, permitiendo proteger las emisiones en cualquier banda de frecuencias y permitiendo el uso de cualquier sistema de armas que utilice el espectro para transmitir y recibir información, guiar armamento y/o accionar contra las amenazas.

Por otra parte, y bajo la perspectiva de Jonás Kjellén (2018) la EW en las FAs rusas, se encontraría organizada en cuatro áreas o campos

de acción, las que se detallan en la Tabla 1: ataque electrónico, protección electrónica, contramedidas contra medios de reconocimiento técnico y, medidas de apoyo de información radioelectrónica.

Tabla 1

Áreas o campos de acción de la Guerra Electrónica rusa

ATAQUE ELECTRÓNICO	PROTECCIÓN ELECTRÓNICA	CONTRAMEDIDAS CONTRA MEDIOS DE RECONOCIMIENTO TÉCNICO	MEDIDAS DE APOYO DE INFORMACIÓN RADIOELECTRÓNICA
• Ataque funcional. • Contramedidas electrónicas. • Misiles antiradiación. • Simulación y decepción electrónica.	• Protección contra ataque electrónico. • Compatibilidad Electromagnética.	• Reconocimiento técnico.	• Reconocimiento técnico (radio, radar, optrónica, acústica e hidro acústico. • Control integral técnico.

Nota: Elaboración propia, basada en estudio de Jonas Kjellén, Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces, 2018.

En relación con el *Ataque Electrónico*, se encuentra el *Ataque Funcional*, que corresponde a un campo secundario, que se caracteriza por el desarrollo de capacidades para destruir elementos electrónicos y por la capacidad de operar en redes de datos, a través de virus y ataques informáticos (Bueno, 2019), lo que en occidente es conocido como Actividades Ciberelectromagnéticas (CEMA). En segundo lugar, las *Contramedidas Electrónicas*, a través de la perturbación afectan los sistemas de mando y control y telecomunicaciones del enemigo, incluyendo la capacidad de destruir dispositivos electrónicos (Kjellén, 2018). Como tercer elemento, los Misiles *Antirradiación*, que a pesar de

ser de antigua data, son una reciente incorporación al arsenal ruso, que busca degradar los sistemas adversarios y proteger los propios, a través del empleo de fuegos letales (Kjellén, 2018). Por último, la simulación y decepción electrónica, es aquella función que busca lograr el engaño electrónico, a través de la interceptación y suplantación de miembros de redes de comunicaciones, además de ser usada para simular y engañar a sistemas de navegación y radares, entre otros. Los efectos que buscaría el ataque electrónico son transversales a todos los niveles de la conducción militar y estarían relacionados con negar el acceso a la información y/o degradar sus sistemas de mando y control (Roderick, 2021).

Sobre la *Protección Electrónica*, es posible identificar en este campo las mayores similitudes con la visión de occidente, ya que se centra en proteger las emisiones propias y permitir así la disponibilidad de los medios propios (Kjellén, 2018). A través de la *Protección contra Ataques Electrónicos*, que, a los procedimientos comunes, suma el empleo de equipos con capacidad para atacar y destruir equipos electrónicos para así proteger los propios, y a la *Compatibilidad Electromagnética*, que se encarga de evitar las interferencias mutuas para permitir la disponibilidad y empleo de los propios medios. Esto se puede sintetizar, en que la Protección Electrónica cumple las mismas funciones de la versión proporcionada por las doctrinas de referencia para nuestro país, pero en las FAs rusas incluye la capacidad de ataque y destrucción como parte de la búsqueda de la supervivencia de los propios sistemas.

En cuanto a las *Contramedidas contra medios de*

reconocimiento técnico, estás se centrarían en impedir que los medios de obtención del enemigo accedan a información que genere grave daño en poder de la voluntad opuesta, ya que, con la degradación y/o afectación de los sistemas de armas, infraestructura crítica de mando y control, y/o puestos de mando, podría afectar el Centro de Gravedad (CoG) propio de una manera indirecta (Kjellén, 2018).

Por último, *las Medidas de apoyo de información radioelectrónica*, corresponden a aquellas que generan las condiciones para que el Ataque Electrónico, la Protección Electrónica y las Contramedidas contra medios de reconocimiento técnico, a través de distintos medios electrónicos que permiten accionar de manera anticipada en el EEM (Kjellén, 2018). Esto permite identificar que los campos de la EW presentados por Jonás Kjellén (2018) son complementarios unos con otro, permitiendo con esto integrar la EW en la Guerra de la Información, operaciones en el ciberespacio y como parte del modelo operacional – táctico empleado por las fuerzas rusas.

Consecuente con la información presentada, para los efectos de este artículo, se considerará la estructura de las Áreas y/o Campos de acción de la Guerra Electrónica rusa expuestos por Kjellen (2018), ya que permitirían abstraerse de la clásica visión occidental, uno de los elementos centrales en los que se basa esta publicación.

Modalidad de empleo

La EW como herramienta que permite lograr efectos en las fuerzas adversarias, propia fuerza y población civil, proporciona

flexibilidad a los comandantes para su empleo. Lo anterior, gracias a que sus acciones dejan poca huella en el terreno, es de alta complejidad atribuir la responsabilidad y, por, sobre todo, actúa en el EEM, componente del campo de batalla moderno que permite actuar en el amplio espectro del conflicto. Algunas de las modalidades que se pueden identificar en las FAs rusas, se presentan a continuación.

Como parte de la ***Guerra Asimétrica***, la EW rusa actúa por su bajo costo en relación con los sofisticados sistemas de armas y de Mando y Control, logrando con sus efectos, altas repercusiones en lo físico y en el ambiente de la información (Roderick, 2021). Esto lo relaciona al mismo tiempo, con el Conflicto Híbrido, impactando en los niveles Estratégico, Operacional y Táctico de la Conducción Militar.

En el marco de la ***Guerra de la Información (IW)***, las FAs rusas, consideran a la Información como el Centro de Gravedad (CoG) de las fuerzas adversarias, permitiendo afectar aspectos claves como la moral, espíritu de lucha de las fuerzas y población del adversario (Bueno, 2019). De lo anterior, es posible concluir que el empleo de la EW permitiría a Rusia nivelar la balanza y acortar las brechas con las tecnologías empleadas por occidente, en especial Estados Unidos y los integrantes de la Organización del Atlántico Norte (OTAN), relacionándose directamente con la modalidad asimétrica.

En relación con las unidades de ***Apoyo de Fuego y técnicos***, Grau y Bartles (2016), exponen que las unidades de EW rusas y en particular las unidades del Ejército de ese país se vincularían con las unidades de artillería, tanto como para reunir información de posibles

blancos, a través de la Inteligencia de Señales y para proteger sus sistemas de información y de localización (GNSS). Del mismo modo, existe una cercana relación con las unidades de telecomunicaciones, debido a que las unidades de EW deben realizar la protección de las propias redes de comunicaciones y, además, del empleo permanente de las comunicaciones entre las unidades de Guerra Electrónica y los Puestos de Mando donde se remite la información obtenida sobre el adversario, blancos y sus sistemas. De estos antecedentes, identificamos una similitud de empleo y conceptual con las funciones de combate de los niveles táctico y operacional de las doctrinas de referencia para nuestro país (EE.UU. y OTAN), como son la función, Inteligencia, Fuegos y Protección.

Sobre su participación como parte del ***Sistema Antiacceso y Denegación de Área (A2/DA)***, la Guerra Electrónica tiene un papel protagónico para lograr los efectos deseados de bloquear el acceso y denegar el control de espacios al adversario. Lo anterior, gracias a que las tareas tienen poca percepción por parte de las unidades que se constituyen en blanco de sus acciones. La versatilidad de la EW queda en evidencia en que es posible proteger a la fuerza a través del control de emisiones y del mismo modo, degradar el sistema de Mando y Control adversario, en especial el sistema de telecomunicaciones como los sistemas de posicionamiento en el terreno. El máximo de efectos, se logran en combinación con fuegos letales y en especial con ciberoperaciones (CEMA), las que en la actualidad se encuentran plenamente integradas (Bueno, 2019). Como conclusión, podemos

identificar que nuestra realidad regional y local, se encuentra limitada en este tipo de empleo, ya que requiere de un amplio desarrollo tecnológico, personal entrenado y una alta disponibilidad de material con el propósito de impedir la acción de fuerzas hostiles en cualquiera de los dominios conocidos.

Por último, se expone la modalidad de empleo como ***instrumento de acción en la llamada Zona Gris*** (Bueno, 2019), esto debido a que los ataques realizados en y a través del espectro electromagnético; al igual que en el Ciberespacio; presentan la dificultad para identificar y localizar al emisor. Es precisamente esta característica la que permite emplear a la EW en la Zona Gris, ya que puede operar desde los orígenes del conflicto, a partir la Crisis como parte de la maniobra en esta etapa, o en el empleo de las capacidades militares en el empleo del potencial bélico. En consecuencia, el uso de la EW daría la posibilidad de lograr efectos desde mucho antes que se inicien las hostilidades, asestando golpes silenciosos y de alta repercusión desde el más alto nivel de la conducción hasta el soldado en el terreno, mezclando lo regular con lo irregular, transitando por la delgada línea del Derecho Internacional de los Conflictos Armados, elemento que ha distinguido a las operaciones rusas en Estonia (2007), Georgia (2008), Siria (2010) y Crimea (2014).

Unidades de EW rusas

Considerando el estudio realizado por Evan Roderick (2021), las unidades de Guerra Electrónica rusas se encontrarían presentes desde

el nivel Teatro de Operaciones hasta el nivel Táctico con el propósito de negar el acceso a cualquier tipo de información por parte del adversario (Roderick, 2021). En el mismo orden de ideas, las unidades de EW estarían compuestas por compañías, batallones y brigadas especializadas. Estas últimas podrían apoyar en cualquiera de los niveles de la conducción militar buscando obtener la iniciativa en el EEM.

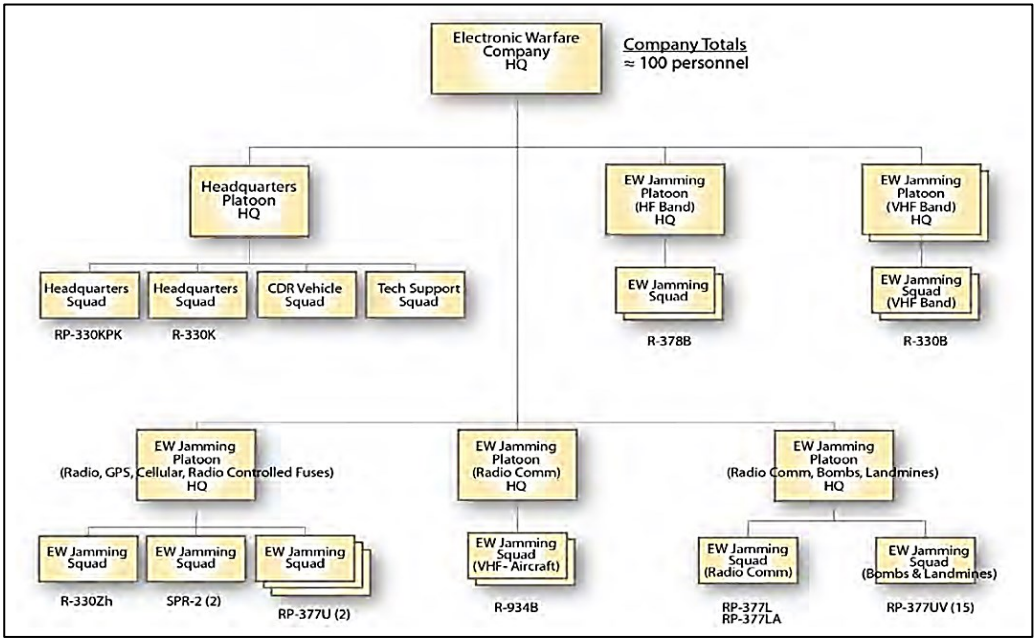
En relación con las unidades de EW; bajo la concepción rusa; las brigadas de Guerra Electrónica; que se encuentran dotadas con batallones; serían empleadas para afectar a objetivos en el nivel estratégico y operacional, integrando material para accionar en el EEM, como así también en combinación con ciberoperaciones, que en cierta medida permiten homologar las acciones realizadas por Estados Unidos y otros países de referencia occidental, conocidas como actividades ciberelectromagnéticas (CEMA), que permiten lograr efectos en estas dimensiones. Estas brigadas contarían con material para atacar electrónicamente las redes de telefonía celular, alterar los sistemas de localización (GNSS) y sistemas de comunicaciones satelitales (Grau y Bartles, 2016).

Pasando al nivel táctico, es posible identificar a las compañías de EW (Figura 2), que se encuentran encuadradas en las Brigadas de maniobra del Ejército ruso. Estas unidades están dotadas con la capacidad de realizar ataques electrónicos (Jamming) en diferentes bandas de frecuencias, incluyendo GNSS y los sistemas de control y de dirección del tiro de las unidades de artillería adversarias (Grau y Bartles, 2016, p.289). Relacionado con el ámbito de las capacidades, estas se

centrarían en interferir, interrumpir y radiolocalizar las emisiones de las fuerzas adversarias.

Figura 2

Compañía de Guerra Electrónica del Ejército ruso



Nota: Informe de Grau y Bartles. The Russian way of war: force structure, tactics and modernization of The Russian Ground Forces. Foreing Military Study Office (FMSO). Fort Leavenworth, KS, USA. (2016).

Experiencias del empleo de las unidades de EW en el conflicto ruso – ucraniano

Después de los antecedentes entregados y contando con una visión general de la Guerra Electrónica rusa, estamos en condiciones de

analizar y extraer experiencias positivas y negativas del empleo de las unidades de EW desde una perspectiva terrestre durante el año 2022, para lo anterior, se presentan hechos ordenandos cronológicamente del período en evaluación.

Experiencias Positivas

Bloqueo de los sistemas de defensa aérea ucranianos

En las primeras horas de la ofensiva; el 24 de febrero de 2022; las unidades tácticas de EW rusas, bloquearon los dispositivos de alerta temprana del sistema antiaéreo ucraniano, desplegados cerca de la frontera (Jones, 2022). Esto como parte de las tareas que buscaban neutralizar el sistema de defensa aérea en Ucrania. La acción antes descrita habría sido complementada con drones de EW que lograron la decepción electrónica de los sistemas ucranianos y la perturbación de los equipos de los sistemas de telecomunicaciones desplegados, impidiendo la reacción de los medios aéreos sobre las unidades terrestres rusas que avanzaban (Jones, 2022).

El empleo de estas unidades habría logrado en primer lugar, el bloqueo temporal de la defensa aérea ucraniana en el teatro de operaciones, permitiendo la acción táctica de la fuerza aérea rusa y, en segundo lugar, el engaño; elemento fundamental en la Guerra; que generaría las condiciones para asegurar el avance de los medios terrestres rusos. En Efecto, constituye un ejemplo de cómo acciones del nivel táctico coadyuvaron al esfuerzo conjunto.

Empleo de unidades de EW en apoyo a la ofensiva en marzo de 2022 en el norte y este de Ucrania

Después del primer mes del conflicto y conforme con las dificultades presentadas en los frentes norte y oeste con Ucrania, el General Gerasimov, Jefe del Estado Mayor de las FAs rusas, dispuso el empleo de las unidades de EW, en específico de Batallones y Brigadas con el propósito de lograr el control del EEM en los frentes antes mencionados para generar las condiciones que asegurarán la ofensiva rusa (Atalayar, 2022). Las unidades desplegadas en el nivel táctico permitieron buscar, identificar, bloquear y perturbar las comunicaciones en las bandas militares (HF/VHF/UHF) de las fuerzas ucranianas en los citados frentes, afectando las comunicaciones satelitales, empleo de radares, redes de telefonía celular, entre otros (Atalayar, 2022). De los antecedentes recopilados, es posible identificar que con el empleo de las unidades de EW se habría logrado la superioridad en el espectro electromagnético por parte de las fuerzas rusas, generando las condiciones para el empleo de las unidades de maniobra, proporcionando el apoyo técnico a las unidades productoras de fuego, a través de los sistemas de navegación y de los diferentes sensores y radares asociados a estos sistemas de armas, constituyéndose en un multiplicador de efectos en el campo de batalla.

Modificación del dispositivo de las unidades de Guerra Electrónica en el frente con Ucrania

Para fines de 2022, las FAs rusas, con las experiencias obtenidas del empleo de medios de Guerra Electrónica en el ámbito táctico y operacional, modificó su despliegue en el terreno, pasando a cubrir con las unidades especialista un frente de 10 Km cada una y una profundidad de 7 Km de distancia hacia el borde delantero (Watling y Reynolds, 2023). Esta modificación optimizaría la cobertura y explotaría en mejor manera las capacidades de las unidades de EW rusas, reduciendo el número de unidades dadas de baja y/o inutilizadas por la acción de las fuerzas de defensa ucranianas. Esta variación del dispositivo se ve respaldada en la evaluación de las operaciones, ya que, en los meses de octubre, noviembre y diciembre de 2022 solo se perdieron 16 plataformas de Guerra Electrónica rusas, lo que en comparación con las 13 bajas de este material solo en septiembre de 2022 (Molfar Global, 2023), permiten concluir que la modificación del dispositivo habría permitido proteger a las fuerzas empleadas.

Empleo de la Guerra Electrónica (EWO) contra drones

De acuerdo con el avance de la guerra, para fines de diciembre de 2022, la Guerra Electrónica rusa logró la destrucción de 90% de los drones o vehículos no tripulados de las fuerzas ucranianas (Axe, 2022), que, para esa altura del conflicto, se habían transformado en una de las principales amenazas para las fuerzas del Kremlin. Lo anterior, fue

investigado por la Revista Forbes a fines del año 2022, que accedió a altos mandos ucranianos, los cuales confirmarían que el 90% de los drones de inteligencia y adquisición de blancos desplegados en el frente con Rusia habrían sido degradados y/o afectados por los ataques electrónicos rusos.

El empleo de las unidades de EWO habría logrado el efecto de suprimir las comunicaciones y los sistemas de localización, permitiendo el derribo de estos medios, ya sea por la acción de la energía electromagnética o por los sistemas productores de fuegos letales (Axe, 2022).

La EW rusa habría logrado degradar a lo menos unas 10.000 unidades de drones por mes desde que comenzó el conflicto (RUSI, 2023). Esta sorprendente cifra, deja de manifiesto la importancia que ha significado para Rusia el contar con este tipo de material, el cual viene sirviendo desde la Guerra contra Georgia en 2008, explotando el máximo de sus capacidades en la guerra contra Ucrania en Crimea en 2014.

De la modalidad de empleo expuesta con relación a la acción de las EWO contra drones y vehículos aéreos no tripulados, se puede obtener la experiencia que la Guerra Electrónica constituiría una herramienta altamente eficaz en contra de este tipo de amenazas, facilitando su búsqueda, interceptación, localización e identificación, lo que, complementado con el uso de armas letales, ha significado una solución para los mandos rusos.

Experiencias Negativas

El Sistema de Mando y Control e infraestructura crítica ucraniana no habrían sido degradados al inicio de la ofensiva rusa.

Antes de comenzar la ofensiva el 24 de febrero de 2022, las FAs rusas ejecutaron acciones de Guerra Electrónica sobre blancos ucranianos del sistema de mando y control, telecomunicaciones y también, afectando la infraestructura crítica (IC) de comunicaciones (Jones, 2022), pero estos no habrían sido degradados lo suficiente como para interrumpir las comunicaciones y/o afectar la voluntad de lucha de las unidades de combate ucranianas. Del mismo modo, la infraestructura crítica que fue objeto de las operaciones de Guerra Electrónica no impidió el funcionamiento de los servicios básicos, logística, transporte público, entre otros. Lo anterior, se puede comparar con otras campañas realizadas por las fuerzas rusas de manera previa, como en Georgia en 2008 donde gracias a la combinación de medios de EW y ciberoperaciones se logró degradar el sistema eléctrico, financiero y de transportes (Nichol, 2012).

El efecto de no haber degradado de manera significativa la IC y los sistemas de mando y control ucranianos al inicio de la ofensiva rusa, traería como consecuencia que los diferentes mandos de la cadena ucraniana continuaran conduciendo a sus unidades. A su vez, la infraestructura crítica, seguiría disponible para el empleo de la ciudadanía y fuerzas militares, las que mantuvieron una alta voluntad de lucha, alargando la temporalidad de las operaciones y dificultado el

avance de las fuerzas rusas hacia las principales ciudades.

Del caso expuesto de manera precedente, se puede obtener la experiencia que no solo se deben afectar, por el contrario, se debe buscar degradar el Sistema de Mando y Control adversario, en los diferentes niveles de la conducción, con el propósito de dislocar la capacidad de toma de decisiones, disminuir la capacidad de obtención de información y principalmente, afectar el entendimiento situacional de los comandantes. Por otra parte, el no degradar infraestructura crítica del adversario con el apoyo de medios de Guerra Electrónica, habría permitido que las fuerzas ucranianas no vieran afectada su voluntad de lucha, un elemento que ha sido distintivo en el esfuerzo de guerra del país.

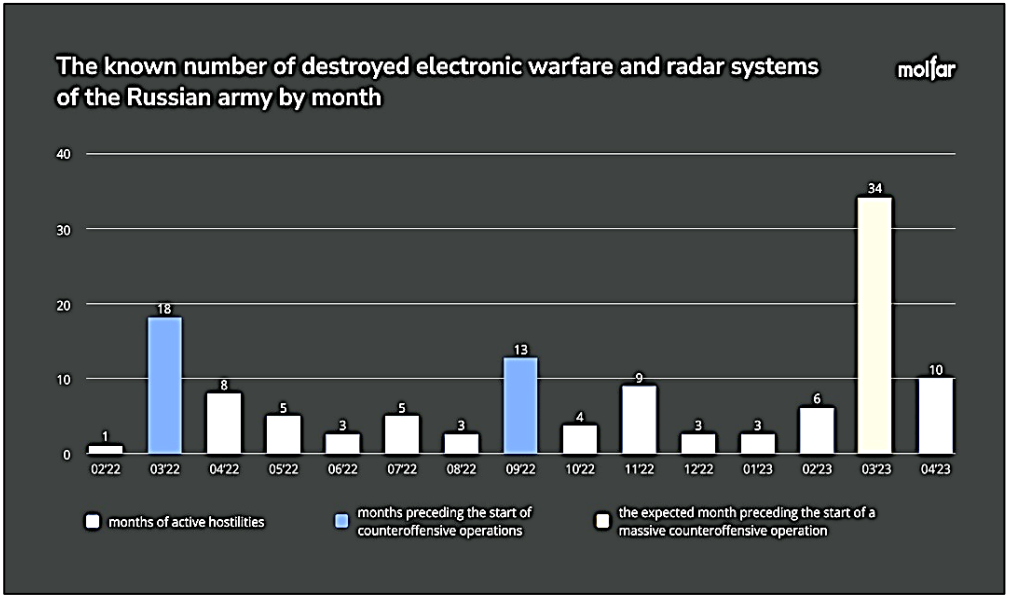
Concentración de unidades de Guerra Electrónica en un solo frente (Donbass)

En el mes de febrero de 2022 se concentró gran cantidad de sistemas de Guerra Electrónica en la región del Donbass (Watling y Reynolds, 2023), lo que implicó reunir en un solo frente gran parte de las capacidades de búsqueda, identificación y localización de emisiones, además de las principales unidades de ataque electrónico. Esto, además de entregar la libertad del empleo del EEM a las fuerzas ucranianas en otros frentes, provocaría la destrucción de un total de 19 sistemas de EW (Imagen N.º 1), teniendo como efecto el generar las condiciones tanto en el espectro electromagnético, como en el ciberespacio para la contraofensiva ucraniana en Kharkiv y Kiev (Molfar Global, 2023). Conforme con lo investigado, se puede concluir que el error en el empleo

de las unidades de EW rusas, habría estado en concentrar gran parte de las capacidades en una zona, no dando frente y profundidad al dispositivo de estas unidades, lo que traería como consecuencia la perdida de medios de obtención de información y unidades productoras de fuegos no letales, extendiendo el tiempo de las operaciones y perdiendo la iniciativa en el espectro electromagnético.

Imagen 1

Cantidad de sistemas de radar y EW destruidos del Ejército ruso



Nota: Reporte de Molfar Global, Destruction of electronic warfare equipment as a prelude to a counteroffensive. Analytics confirms dates of counteroffensive announced by the Ministry of Defense of Ukraine (2023).

Abandono de material de Guerra Electrónica en el terreno

Durante el mes de marzo de 2022; cuando ya el avance a Kiev se hacía cada día más complejo; las fuerzas terrestres rusas, acercaron las unidades de Guerra Electrónica al frente contra Ucrania, estas cuentan con material Krasukha – 4 (Imagen 2), un sistema de EW con la capacidad de interferir las señales de satélite, comunicaciones, radares y armas inteligentes (Clark, 2022). Debido a las características del terreno, las condiciones atmosféricas en ese frente y la tenaz resistencia de las fuerzas ucranianas provocaron que las fuerzas rusas dejaran abandonado en el terreno uno de sus principales sistemas de EW. De este ejemplo, es posible identificar que el adelantar las unidades de EW a la frontera este de Ucrania, sin haber generado las condiciones de seguridad y de conectividad que permitieran su desplazamiento y protección, habrían tenido un impacto directo sobre la disponibilidad de este material, terminando abandonado en el campo de batalla, proporcionando información de alta sensibilidad al adversario, afectando el futuro empleo de estas unidades especializadas.

Imagen 2

Sistema de EW ruso Krasukha – 4 capturado por el Ejército ucraniano

Nota: Reportaje ABC Internacional,Ucrania captura uno de los sistemas de guerra electrónica más avanzados de Rusia (2022).

Baja de altos mandos rusos por acción de la EW adversaria

Durante el desarrollo de las operaciones y con el despliegue de los Puestos de Mando de los distintos niveles de la conducción de las fuerzas armadas rusas, aumentaron las emisiones electromagnéticas, las cuales por una parte han permitido sustentar las comunicaciones de los medios desplegados, por otra parte, constituyen una amenaza para el ocultamiento del despliegue de las fuerzas y su protección.

Como parte de la acción de la Guerra Electrónica empleada por las fuerzas ucranianas, encontramos en las operaciones realizadas en el

año 2022, interceptaciones, localizaciones y ataques electrónicos, que permitieron obtener la ubicación de Puestos de Mando, unidades productoras de fuego, radares de campo de batalla, lo que permitió asestar duros golpes a los Sistemas de Mando y Control y fuego rusos.

Evidencia de lo anterior, lo constituye la muerte del Teniente General Andriy Mordvichev; comandante del 8º ejército del Distrito Militar del Sur de la Federación Rusa; en marzo de 2022; en un ataque realizado al aeródromo en Chornobayivka (ABC Internacional, 2022). Esto gracias a la acción de la EW ucraniana, ya que lo habrían localizado gracias a una llamada a su teléfono móvil, logrando identificar su ubicación, informando al alto mando de las FAs ucranianas, que determinarían el batimento de este objetivo de alto valor.

Por otra parte, debemos mencionar la baja del General Andrei Simonov (Imagen 3) el 30 de abril de 2022; Comandante de la Guerra Electrónica rusa; junto a otros 100 soldados rusos en Izium, en un ataque realizado sobre el Puesto de Mando del 2do Ejército ruso ubicado en la región de Járkov en el este de Ucrania, gracias al empleo de unidades de EW ucranianas (El Periódico, 2022). Estas habrían confirmado la ubicación de las instalaciones, sincronizándose con las unidades productoras de los fuegos operacionales, las cuales asestarían este duro golpe al alto mando ruso. Del mismo modo, existen antecedentes que el Jefe de Estado Mayor de las FAs rusas, General Gerasimov, habría resultado herido en dicho ataque, mientras se encontraba conduciendo las operaciones en ese frente (Fernández, 2022).

Los casos antes expuestos, permiten identificar como

experiencia, la poca protección a la fuerza y sistemas de mando y control realizada por las FAs rusas, lo que tuvo como efecto, la pérdida de dos generales y más de 100 soldados altamente especializados, asestando un duro golpe al ciclo de toma de decisiones y a la cadena de mando rusa.

Imagen 3

General Ruso Andrei Simonov

Nota: Reportaje La Razón, *Así es como Ucrania ha matado a doce generales rusos desde su cuartel móvil*, (2022).

Conclusiones

En relación con la investigación desarrollada sobre el empleo del espectro electromagnético durante la "Operación Militar Especial Rusa", se presenta al lector una síntesis con los elementos que fueron identificados en el proceso.

En primer lugar, se realizó una revisión de la concepción de la EW rusa, la cual, a diferencia de la versión occidental, se centra en la información, permitiendo identificar su vinculación con las INFOOPS y la IW. Del mismo modo, se pudo ver el papel que jugaría la Guerra Electrónica bajo el paradigma de la Doctrina Gerasimov, actuando de manera integrada en todos los niveles de la conducción militar en acciones convencionales y no convencionales.

Seguidamente, en el proceso de identificación de las actividades y áreas de la EW rusa, fue posible apreciar que la inclusión de la capacidad de destrucción física de los equipos electrónicos a través del EEM, aumentarían el grado de protección de la fuerza y su incorporación a los medios productores de fuegos letales.

Posteriormente, fueron observadas las modalidades de empleo de la EW, destacándose: su empleo en la Guerra de Información, como parte de los medios de apoyo de fuego y técnicos, en el Sistema Antiacceso y Denegación de Área (A2/DA) y como un instrumento para usar en la Zona Gris. De todas estas, el factor común es que la EW proporcionaría una flexibilidad para actuar sola o en compañía de ciberoperaciones con el propósito de maximizar esfuerzos, aprovechando que su característica principal es que es difícil identificar al autor de estos ataques.

Desde una perspectiva general, se pueden establecer que la EW en el nivel táctico, si bien provee una capacidad poderosa y con potencial de influir en el resultado, sus efectos son locales y transitorios, lo que debe ser considerado en la planificación. Por otra parte, si las

condiciones del terreno son propicias, las unidades de EW pueden redirigir su accionar y efectos a objetivos de forma rápida y ágil, permitiéndoles apoyar en un frente extendido. En consecuencia, considerando las experiencias positivas y negativas del empleo de las unidades de EW en el conflicto ruso – ucraniano durante el año 2022, se pudieron obtener las siguientes conclusiones:

Comenzando con las ***experiencias positivas***, se analizó el empleo de unidades de EW en contra de los sistemas de defensa aérea, quedando en evidencia que, su principal aporte está en generar las condiciones para el empleo de las unidades de maniobra y del mismo modo, en ayudar a lograr el engaño y ocultamiento de las propias intensiones, proporcionando seguridad al dispositivo y a las fuerzas propias.

A su vez, como un elemento de apoyo a la ofensiva en el frente norte y oeste ucraniano, se pudo identificar que las unidades de EW son idóneas para emplear en la configuración del campo de batalla, sumando incertidumbre al ciclo de toma de decisiones del adversario a través de la afectación de los sistemas de comunicaciones, navegación y sistemas de adquisición de blancos adversarios.

Un acierto importante en relación con el empleo de las unidades de EW lo constituye la modificación realizada al dispositivo de las unidades en el frente con Ucrania, ya que, para fines del año 2022, estas se desplegarían con un frente de 10 Km y una distancia de 7 Km al borde delantero, lo que le proporcionaría mayor seguridad y protección y por sobre todo mayor coordinación, ya que se reducirían los números de

bajas y las propias unidades afectadas por las acciones de EW rusas.

El empleo de la EW contra los drones ucranianos constituye una solución eficaz contra este tipo de amenazas, facilitando la búsqueda, interceptación, identificación y localización de estos elementos y su posterior destrucción. *Este empleo a juicio del autor es la principal experiencia que se podría ocupar en nuestra realidad nacional*.

De las ***experiencias negativas***, en primer lugar, se identificó la necesidad de degradar los sistemas de Mando y Control y la IC adversarios, en el inicio de las operaciones en desmedro de solo afectar, ya que al degradar se denegaría el acceso a la información y a ciertos servicios por períodos más extensos de tiempo, permitiendo generar las condiciones para la acción de las unidades de maniobra y fuegos.

En el mismo orden de ideas, el concentrar un gran número de unidades de EW en el frente del Donbass, permitió una alta tasa de destrucción de este tipo de unidades, que requieren de personal especialista y ocupan sistemas de alta complejidad, difíciles de reemplazar, constituyendo uno de los principales desaciertos durante el 2022 por parte de las FAs rusas.

El abandono de material de EW en el terreno durante el año 2022, a pesar de que obedece a procedimientos, el destruir este tipo de equipamiento, deja la experiencia que no se puede dejar en el terreno equipamiento que proporcione información de alta sensibilidad al adversario. Esto viene a confirmar la falla del sistema de contrainteligencia, procedimientos y controles internos de las FAs rusas.

Como última experiencia y con el ejemplo de la baja de dos

generales del alto mando ruso, dejan de manifiesto que a pesar de contar con alta tecnología en EW, las FAs no habría aplicado los protocolos vigentes. Ya que, producto de una simple llamada por celular fue localizada la ubicación de uno de estos altos oficiales, provocando su muerte. Aquí es posible identificar una tremenda experiencia con relación a la seguridad, protección de la fuerza y medidas de contrainteligencia que se deben complementar con las capacidades propias de EW y con principal atención en las del adversario.

Finalmente, el desafío de obtener experiencias de este conflicto, continua de manera evolutiva, ya que serán los años los que nos permitirán continuar empleando esta guerra para el aprendizaje y como laboratorio de estudio que permita aportar a la formación de los futuros oficiales de Estado Mayor.

Referencias Bibliográficas

ABC Internacional. (2022). Ucrania captura uno de los sistemas de guerra electrónica más avanzados de Rusia. En https://www.abc.es/internacional/abci-ucrania-captura-sistemas-guerra-electronica-mas-avanzados-rusia-202203271705_noticia.html.

ABC Internacional. (2022). Ucrania mata a un general ruso después de que hiciera una llamada no segura que les dio su ubicación. En https://www.abc.es/internacional/abci-ucrania-mata-general-ruso-despues-hiciera-llamada-no-segura-ubicacion 202203231033_noticia.html.

Atalayar. (2022). La invisible y desconocida guerra electrónica que se libra en Ucrania. En https://www.atalayar.com/articulo/nuevas-tecnologias-innovacion/la-invisible-y-desconocida-guerra-electronica-que-se-libra-en-ucrania/20220314092255155512.html.

Axe, David. (2022). Russia's Electronic-Warfare Troops Knocked Out 90 Percent Of Ukraine's Drones. En https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?sh=157abce4575c.

Bueno, Francisco. (2019). Guerra Electrónica: La gran ventaja rusa. En Revista Digital. En https://www.revistaejercitos.com/2019/11/18/guerra-electronica-la-gran-ventaja-rusa/

Clark, David. (2022). The Fall and Rise of Russian Electronic Warfare: The Ukraine invasion has become an old-fashioned slog, enabling Russia to unleash its electronic weapons. Obtenido de

https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare.

Department of the Army. (2021). FM 3 – 12 “Cyberspace operations and Electromagnetic warfare”. Washington DC, EUA: HQ Department of the Army.

Ejército de Chile, (2022). Reglamento de Guerra Electrónica. Santiago, Chile: División Doctrina.

NFernández, Antonio. (2022). Así es como Ucrania ha matado a doce generales rusos desde su cuartel móvil. En periódico en línea La Razón https://www.larazon.es/internacional/20220505/nyf6mzvquzc7de6chmgzqkpjoe.html.

Grau, Lester y Bartles, Charles. (2016). The Russian way of war: force structure, tactics and modernization of The Russian Ground Forces. Foreing Military Study Office (FMSO). Fort Leavenworth, KS, USA.

Jones, Seth. (2022). Russia’s Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare. En CSIS Briefs (Center for Strategic & International Studies). https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare.

Kjellén, Jonas. (2018). Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces. Stockholm, Sweden: Swedish Defence Research Agency.

Masalleras, Marcelo. (2022). Rusia, Ucrania y la Doctrina Gerasimov. En AthenaLab. Santiago, Chile: AthenaLab.

Molfar Global. (2023). Destruction of electronic warfare equipment as a prelude to a counteroffensive. Analytics confirms dates of

counteroffensive announced by the Ministry of Defense of Ukraine. En https://www.molfar.global/en-blog/electronic-warfare-equipment-of-russian-occupiers.

Nichol, Jim. (2012). The Russo-Georgian War: The Role of the cyberattacks in the conflict. AFCEA INTERNATIONAL.

Roderick, Evan. (2021). New Weapons, New Options: Electronic Attack in Multi-Domain Operations. Fort Leavenworth, KS, USA: School of Advanced Military Studies US Army Command and General Staff College.

Turunen, Adreas. (2020). The Broader Challenge of Russian Electronic Warfare Capabilities. Washington, USA: Georgetown, University.

Valderrama, Carlos. (1980). Guerra Electrónica. En Revista de Marina Noviembre – Diciembre. Viña del Mar, Chile: Armada de Chile.

Watling, Jack y Reynolds, Nick. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. London, UK: Royal United Services Institute for Defence and Security Studies.