1.7

La Guerra Electrónica y la Ciberguerra en el conflicto de Ucrania

Por el CR Com (R) Ing Mil Rafael Olvieri

«Sé extremadamente sutil hasta el punto de no tener forma.
Sé completamente misterioso, hasta el punto de ser silencioso.
De este modo podrás dirigir el destino de tus adversarios.»
de Sun-Tzu, "El arte de la guerra"

Temario

PALABRAS CLAVE: GUERRA ELECTRÓNICA (EW) – CIBERGUERRA - ESPECTRO ELECTROMAGNÉTICO – CIBERESPACIO – SOFTWARE – HARDWARE – COMANDO Y CONTROL – SISTEMAS DE ARMAS – TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TICS) .

Resumen

El presente artículo describe las características de la guerra actual librada en el espectro electromagnético y en el ciberespacio en el marco de la guerra de Ucrania, como dos espacios intangibles, pero que afectan fuertemente las operaciones en el terreno, y en otros ámbitos como la comunicación, propaganda, gobierno y acción psicológica sobre la población y las tropas.

Introducción - Breves antecedentes del conflicto en Ucrania 2022 y contexto

El conflicto entre Rusia y Ucrania, que se origina en 2014 con la independencia de las regiones del este de Ucrania, con población mayoritariamente de origen ruso, nos muestra un nuevo tipo de gue-

rra, caracterizado por acciones en el campo de batalla, en el espectro electromagnético, en el ciberespacio y en los medios de comunicación social.

Los pueblos de Rusia, Bielorusia y Ucrania, tienen un origen común, de raza eslava, religión católica ortodoxa que formaron parte del imperio ruso y posteriormente de la Unión de Repúblicas Socialistas Soviéticas (URSS), desde donde enfrentaron enemigos comunes. La Ucrania que hoy conocemos fue moldeada en los mismos orígenes de la URSS en tiempos de Vladimir Lenin, de ahí el origen más directo de la escisión territorial del Dombas y Crimea.

Asimismo, estos tres países terminaron decidiendo la disolución de la URSS en la década de 1990.

Finalmente la Federación Rusa termina heredando el poder militar y político de la URSS, y en acuerdo con EEUU y la OTAN (Organización del Tratado del Atlántico Norte) concentra todo el poder nuclear distribuido en la URSS y se firman acuerdos para el desarme de ambas partes y no avance de la OTAN más allá de las fronteras del Pacto de Varsovia, acuerdos que no se cumplen y que se suman a las tensiones que finalmente origina la guerra actual con la invasión rusa de Ucrania el pasado 24 de febrero de 2022.

Se trata de una guerra en el siglo XXI librada por una potencia euroasiática, Rusia, con una doctrina militar particular y un desarrollo social, político, científico y tecnológico propio con conceptos y valores un tanto diferentes al de las potencias occidentales lideraras por Estados Unidos y agrupadas bajo la alianza de la OTAN, y que apoyan abiertamente a Ucrania. Destacamos que este país, la otra parte del conflicto, estuvo ligado a Rusia desde la creación misma del Imperio Ruso, y recientemente como país miembro de la Unión de Repúblicas Socialistas Soviéticas. Por tanto, si bien hoy se ha acercado a Occidente, conoce muy bien la cultura y doctrina militar rusa.

En consecuencia, vemos que la guerra en Ucrania es un conflicto muy complejo, que va más allá de una cuestión política local o territorial. Por este motivo, considero que analizar un aspecto puntual del conflicto se torna complejo, puesto que no recibimos información imparcial. Estamos en Occidente de un lado del conflicto, y muchas notas están marcadas con un sesgo político e ideológico por ambas partes.

No obstante, podemos inferir qué tecnologías y sistemas se estarían empleando en ambos bandos, basados únicamente en publicaciones y noticias, evitando cualquier evaluación categórica, puesto que la guerra está en curso actualmente y parece continuar por un tiempo considerable.

Luego de la caída de la Unión Soviética, Rusia ha rescatado sus valores tradicionales, y la patria histórica, rehusando someterse a las imposiciones de Occidente, y buscando recuperar su lugar y liderazgo geoestratégico. El "fin de la historia" expuesto por Fukuyama en 1992 después de la caída de la URSS, finalmente no sucedió. Sin embargo, a pesar de su vasto territorio y recursos, Rusia no llega a equiparar y menos superar el poder militar y tecnológico de Occidente, por lo cual ha desarrollado doctrinas, armamento y equipos particulares para actuar en un modo asimétrico con sus adversarios, y aún así obtener ventajas.

Por esa razón ha desarrollado muy bien conceptos disruptivos en armamento, como los misiles hipersónicos, mantuvo y renovó un poder nuclear como elemento de disuasión y, desarrolló elementos y doctrinas de guerra electrónica y ciberguerra como un multiplicador de fuerza en el campo de combate y en hostilidades, aun sin llegar a un conflicto armado.

Otro recurso es lo que se conoce como "guerra híbrida", concepto que nace hacia el año 2000, y que incluye otra acciones, como la propaganda, los ciber ataques, acciones en los medios de comunicación social y redes sociales, insurgencias, acciones subversivas en general, que complementan las acciones militares, y pueden realizarse, aún sin conflicto armado.

En esto último entran claramente las acciones realizadas en el ciberespacio.

Esto no es nuevo, lo hace desde la era soviética, donde ya la guerra electrónica era muy impor-

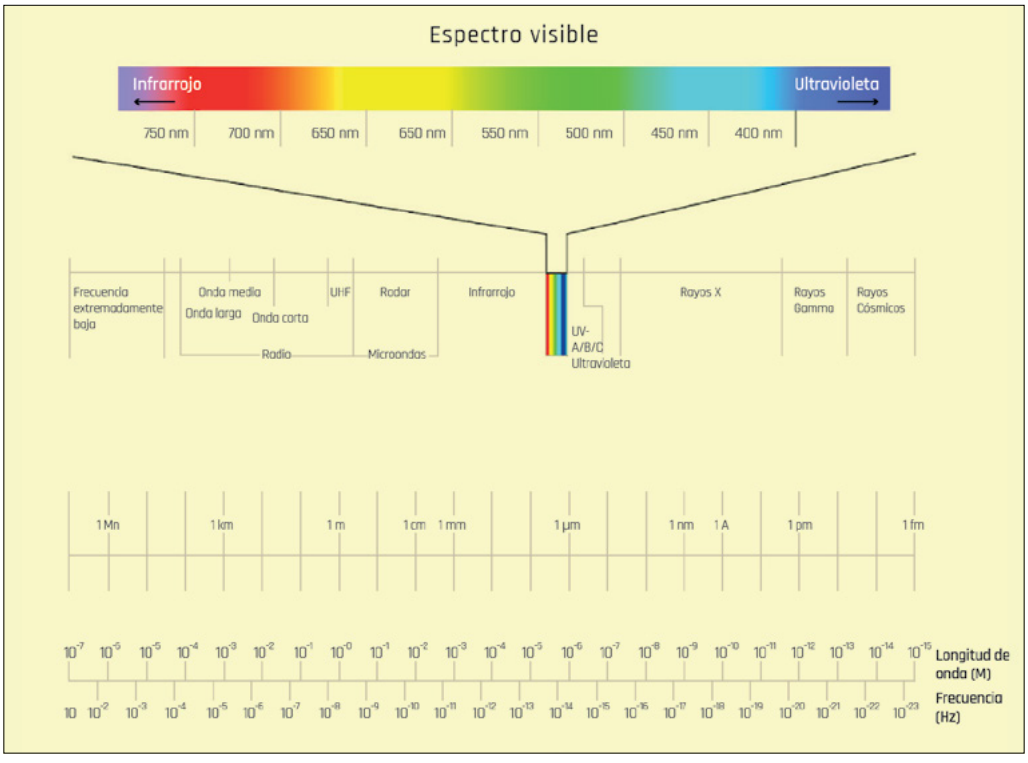
tante en la misma guerra fría y otros conflictos. También las acciones subversivas, aunque no se hablaba en esos tiempos de guerra híbrida. La URSS fomentó siempre el desarrollo tecnológico, como forma de mantener y equiparar su poder con las potencias de occidente, y varios ejemplos lo corroboran, como la carrera espacial. En 1960, logran detectar y derribar un avión espía estadounidense U2 sobre territorio de la URSS. En 1965 en Siria, asesores militares soviéticos empleando medidas de apoyo electrónico, logran radiolocalizar al famoso espía israelí Eli Cohen. Esto entre otras tantas acciones destacadas, marcan una tendencia, que solo se interrumpió durante algún tiempo luego de la caída de la URSS, pero luego continuó, manteniendo Rusia intereses y objetivos de la URSS, como la intervención en Siria y la presencia en otras regiones.

En particular la guerra electrónica es un multiplicador de fuerza que nació a principios del siglo XX, y que el consenso general la ubica en la Batalla de Tsushima durante la guerra entre Rusia y Japón en 1905, y que ha evolucionado hasta hoy con doctrinas, procedimientos y medios. La ciberguerra es otro multiplicador de fuerza, más moderno que algunos reconocen su nacimiento en la década de 1990 del siglo pasado, y rápidamente se proyectó a este siglo XXI junto con la amplia difusión de las computadoras, redes y los dispositivos conectados bajo el concepto de "Internet de las Cosas" (IoT).

Conceptos sobre los sistemas de Guerra Electrónica

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 electromag-

FIGURA: EL ESPECTRO ELECTROMAGNÉTICO.



néticas 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 mediante ondas electromagnéticas, 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 espectro 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 guerra electrónica se divide en tres actividades fundamentales:

Medidas de apoyo de Guerra Electrónica (MAE): comprende las acciones adoptadas para buscar, interceptar, identificar o ubicar fuentes de energía electromagnética irradiada por el enemigo con el objeto de obtener información. Es una acción pasiva, no emite radiación, y sirve para obtener información. Esto proporciona por un lado una fuente de información para inteligencia y, por otra parte, se emplea para ejecutar, si viene al caso operaciones activas de GE sobre el enemigo como la interferencia y el engaño que se describen a continuación.

Contramedidas electrónicas (CME): comprende las acciones adoptadas para impedir o reducir la utilización del espectro electromagnético por parte del enemigo. Estas incluyen básicamente la interferencia para negar el uso del espectro al enemigo o perturbarlo, y el engaño, con el fin de manipular, decepcionar o confundir al enemigo.

Contra Contra Medidas Electrónicas (CCME): o medidas de protección electrónica para asegurar el uso propio del espectro electromagnético frente a las acciones de Guerra Electrónica por parte del enemigo.

Finalmente, se suele clasificar también a la Guerra Electrónica, como Guerra Electrónica de Comunicaciones, que afecta al Comando y Control, y Guerra Electrónica de no-Comunicaciones, que afecta a sensores y sistemas de armas, como radares, defensa aérea, misiles y drones.

Desde hace años, la Guerra Electrónica está incluida en la doctrina de las fuerzas armadas en todo el mundo, si bien los países con menores recursos no la emplean tanto.

Asimismo, el empleo de la guerra electrónica, requiere personal altamente calificado, con sólidos conocimientos técnicos y operativos. El desarrollo de CME y CCME es permanente, si no hay desarrollo los equipos y sistemas de armas se tornan rápidamente vulnerables.

Conceptos sobre 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 más formas, en general basadas en el engaño, y en 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, además de otras acciones más complejas y constituye una importante fuente de información de inteligencia. Se basa 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 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.

Podemos decir que está vinculada a la Guerra Electrónica, por cuanto se puede llegar de una a otra y viceversa. Acciones en el espectro electromagnético pueden afectar al ciberespacio y acciones en el ciberespacio pueden afectar al primero.

Más allá de lo que se difunde cotidianamente en las noticias, sobre ciberseguridad que afectan datos personales, incluyen delitos, espionaje industrial y acciones psicológicas entre otros, la tomaremos aquí en el contexto de un conflicto armado.

Podemos destacar las siguientes características:

i. El ciberespacio es un entorno único, en el que el atacante puede estar en cualquier parte del planeta.
ii. En la defensa intervienen muchos factores, y no sólo elementos estatales sino también privados. Se requiere coordinación entre todos ellos.
iii. La confrontación en el ciberespacio presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.
iv. Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema, y muchas veces sin que la víctima se entere.
v. Permite también ejercer el chantaje; pero, al mismo, tiempo, la defensa puede utilizarlo para la disuasión.
vi. La evolución es rápida siguiendo el avance tecnológico de las tecnologías de la información y las comunicaciones (TIC).

Las acciones que se desarrollan en el ciberespacio, no necesariamente tienen que ocurrir en el contexto de una guerra, ni en el campo de combate mismo, sino que pueden darse en cualquier ámbito y lugar que perjudique al adversario.

La ciberguerra plantea un nuevo entorno operacional, un nuevo campo de combate de la misma entidad que el terrestre, naval o aéreo, que sin duda está siendo empleado en los conflictos actuales, en particular éste, por los países adversarios.[1] Este nuevo entorno, demanda unas nuevas necesidades, entre las que destacan la de una fuerza especializada para operar en él, compuesta por medios dedicados, humanos, físicos y económicos, como lo venimos publicando en diferentes noticias

1 Centro Superior de Estudios de la Defensa Nacional de España – 126 "El Ciberespacio. Nuevo escenario de confrontación.

internacionales en la web de este "Centro de Estudios de Prospectiva Tecnológica Militar General Mosconi"[2].

Con el avance de la ciberguerra, muchos países han elaborado doctrina y elementos de acción en el ámbito de la Defensa para contrarrestar sus acciones, que cada vez son más frecuentes y dañinas.

Por ejemplo, nuestro país cuenta con una Subsecretaría en el Ministerio de Defensa, un elemento conjunto, y elementos en las tres Fuerzas Armadas y otros tantos en las Fuerzas de Seguridad, aunque en estas últimas, más enfocados a los delitos contra personas y entidades, pero como vimos este espacio no tienen límites precisos, en caso de conflictos entre naciones todo debe ser coordinado, incluso las acciones privadas.

Los atacantes y objetivos, no necesariamente han de estar en la zona del conflicto. Un individuo en cualquier parte del mundo puede ser un atacante, para cualquier parte del conflicto, y sin importar su nacionalidad, es un "soldado" anónimo.

Lo mismo podemos decir respecto de los objetivos, por ejemplo, un medio de comunicación o una empresa global de telecomunicaciones en cualquier lugar del mundo puede ser un objetivo, si de alguna manera tiene un vínculo con cualquiera de las partes, y tiene valor un ataque sobre ella.

Con esto, será difícil medir los efectos de la ciberguerra directamente en el campo de combate (marco táctico) como así también en el tiempo propio de ese marco táctico.

Asimismo, al igual que la EW, el empleo de la ciberguerra requiere personal altamente calificado, con sólidos conocimientos técnicos y operativos.

Guerra Electrónica y Ciberguerra en el conflicto

Introducción:

Cuando Rusia agrupó sus tropas en la frontera con Ucrania en febrero de 2022, los analistas especularon con que Rusia comenzaría su asalto con ataques cibernéticos masivos y disruptivos, el equivalente moderno de eliminar defensas mediante bombardeos convencionales. Pero las capacidades de comando y control de Ucrania no se vieron interrumpidas en gran medida, y solo se produjeron interrupciones menores en las funciones gubernamentales.

Sí se produjeron una serie de ataques de distinto tipo sobre la infraestructura crítica y sistemas en red de Ucrania. Abarcando desde sitios gubernamentales, empresas privadas, medios de comunicaciones, infraestructura crítica (electricidad, agua, gas, etc) y telecomunicaciones, según diversos análisis como el del Centro de Estudios Estratégicos e Internacionales[3].

Por ejemplo, según la misma fuente, los ataques de Viasat y Ukrtelecom causaron interrupciones en las comunicaciones, pero aun así no dañaron gravemente la capacidad de Ucrania para coordinar sus fuerzas. Otros sectores sufrieron ataques pero se recuperaron razonablemente rápido.

Algo similar podemos afirmar sobre las acciones de guerra electrónica al inicio de las operaciones, donde parecía poco o nada efectiva en cuanto a anular las capacidades de comando y control de las fuerzas ucranianas y sus principales sistemas de armas.

Pero, ¿la información que recibimos ponderando la defensa ucraniana y señalando la ineficacia de Rusia es tan real o tiene alguna explicación?

La guerra electrónica:

Algunos analistas han señalado que la fase inicial de la guerra en Ucrania no es indicativa de las capacidades EW rusas, ya que la confusión causada por la falta de tiempo de planificación condujo

2 https://www.fie.undef.edu.ar/ceptm/

3 Centro de Estudios Estratégicos e Internacionales: https://www.csis.org/analysis/hidden-war-ukraine

al fratricidio, la mala coordinación de mando y, por lo tanto, muchos sistemas EW rusos se mantuvieron apagados. Posteriormente, las fuerzas armadas rusas comenzaron a utilizar sus capacidades EW de manera más sistemática.

Además, las grandes distancias que cubrió el frente de avance hace que en determinados lugares no se puedan implementar las CCME para defender las tropas propias, y en ese caso pueden operar efectivamente los drones, la fuerza aérea y el apoyo de fuego entre otros, simplemente porque sus sistemas de comando y control y sistemas de armas (en este caso los ucranianos), no pueden ser interferidos por el enemigo.

En este momento, el Ejército ruso está equipado con una variedad de sofisticados sistemas de bloqueo de señales (CCME), incluidos los Krasukha, Moskva, Infauna, Leer y Triad, entre otros.

FIGURA: SISTEMAS RUSOS DE GUERRA ELECTRÓNICA DESPLEGADOS EN UCRANIA

Sistema de guerra electrónica	**Empleo**	**Primer despliegue**	**Notas**
1RL257 Krasukha-4	Apunta a radares de banda X y banda K, particular-mente en aviones, drones, misiles y satélites de órbita baja	2014	Consta de dos camiones KamAZ-6350, uno un puesto de mando y el otro equipado con sensores
1L269 Krasukha-2	Apunta a radares de banda S, particularmente en plataformas aerotransportadas. A menudo se usa junto con el Krasukha-4	2011	También basado en dos camiones KamAZ-6350
RB-341V Leer-3	Interrumpe las comunicaciones VHF y UHF, incluidas las comunicaciones celulares y las radios militares, a lo largo de cientos de kilómetros.	2015	Consiste en un puesto de mando basado en camiones que funciona con drones Orlan-10 para ampliar su alcance
RH-330Zh Zhitel	Interferido o jammer; puede apagar las comunicaciones GPS y satelitales en un radio de decenas de kilómetros	2011	Consta de un puesto de mando de camión y cuatro antenas de matriz en fase de mástil telescópico
Múrmansk-BN	Detección de largo alcance y bloqueo de radios militares HF	2020	Fuentes rusas afirman que puede bloquear las comunicaciones a miles de kilómetros de distancia.
R-934B	Jammer VHF/UHF que apunta a comunicaciones inalámbricas y por cable	1996	Consiste en un camión o un vehículo con orugas y un generador remolcado de 16 kilovatios
SPN-2, 3, 4	Bloqueadores de banda X o K que apuntan a radares aerotransportados y radares de control de guía aire-superficie	(No disponible)	Consiste en un vehículo de control de combate y un vehículo de antena.
Repelent-1	Sistema antidron	2016	Pesa más de 20 toneladas
Moeskva-1	Receptor de precisión HF/VHF para la ubicación coherente pasiva de barcos y aviones enemigos	2015	Las fuentes publicadas citan un alcance de hasta 400 kilómetros.

Publicado por IEEE Spectrum, julio de 2022 - "La caída y el auge de la guerra electrónica rusa ".

Desde el inicio de la guerra se habló en muchos medios y artículos de la ineficiencia del Ejército ruso y de su guerra electrónica, incluso se dijo que un sistema el Krasukha-4 había sido abandonado en la retirada y cayó intacto en manos del ejército ucraniano. De ser cierto, es algo ciertamente muy grave, puesto que se trata de un sistema moderno, diseñado para interferir sistemas de control de tiro de aeronaves y satélites en las bandas Ku y X. Esto afecta a los sistemas estadounidenses E-8 Joint Surveillance Target Attack Radar System (JSTARS) y Airborne Warning and Control System, (AWACS).

En ese caso Ucrania, y sus socios de inteligencia de la OTAN, tendrían un Krasukha-4 para diseccionar y analizar. Algo muy valioso en la guerra, similar a la captura por parte de los aliados de una máquina Enigma en la 2da Guerra Mundial.

FIGURA: EL COMPLEJO "REPELLENT" ESTÁ DISEÑADO PARA EL RECONOCIMIENTO ELECTRÓNICO DE VEHÍCULOS AÉREOS NO TRIPULADOS QUE UTILIZAN SEÑALES DE SISTEMAS ELECTRÓNICOS Y SUPRIMEN SUS SISTEMAS DE CONTROL.

Fuente: Rosoboronexport.

FIGURA: SISTEMA KRASUKHA-4

Fuente: https://www.armyrecognition.com/russia_russian_military_field_equipment/

Por ejemplo, el bloqueador ruso R-330Zh Zhitel puede interferir, dentro de un radio de decenas de kilómetros, las redes de GPS, comunicaciones por satélite y telefonía celular en las bandas VHF y UHF. También tiene capacidad de engaño, en el que un sistema sustituye su propia señal por una transmisión de radio o radar esperada. Con esto, las fuerzas rusas enviaron propaganda y órdenes falsas a tropas y civiles durante la insurgencia de 2014 a 2022 en el este de Ucrania mediante el secuestro de la red celular local con el RB-341V Leer-3.

También, antes de la guerra, buques mercantes que navegaban en el Mar Negro, denunciaron comportamientos anómalos de los sistemas GPS que indicaban posiciones incoherentes con el lugar.

Empleando drones Orlan-10 controlados por un sistema montado en un camión, el Leer-3 puede extender su alcance e impactar las comunicaciones VHF y UHF en áreas más amplias.

En cuanto a las capacidades MAE (pasivas), unos pocos sistemas rusos como el Moskva-1 , que es esencialmente un receptor HF/VHF de precisión que puede emplear los reflejos de las señales de radio y televisión para realizar operaciones pasivas de ubicación coherente o de radar pasivo. Este

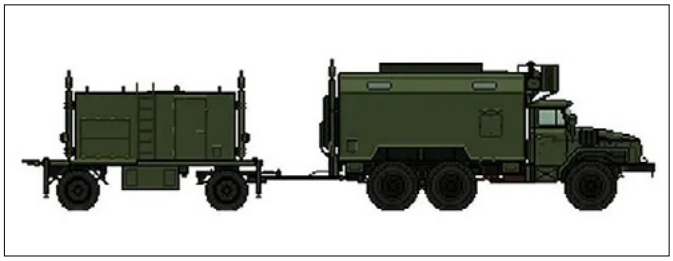
sistema capta las transmisores de radio y televisión comerciales en un área, que se reflejarán en objetivos como barcos o aviones. Mediante la triangulación entre múltiples conjuntos de ondas recibidas, el objetivo puede identificarse con suficiente precisión para rastrearlo y, hasta batirlo con fuego de artillería.

Rusia emplea unidades especializadas en guerra electrónica para ejecutar MAE y CCME. En sus fuerzas terrestres , se asignan brigadas EW dedicadas a los cinco distritos militares rusos (oeste, sur, norte, centro y este) para apoyar las operaciones EW regionales que incluyen la interrupción de los radares de vigilancia enemigos y las redes de comunicación satelital en cientos de kilómetros. Las brigadas EW están equipadas con los sistemas más grandes Krasukha-2 y Krasukha-4, Leer-3, Moskva-1 y Murmansk-BN (este último detecta e interfiere las radios HF). Cada brigada del ejército ruso también incluye una compañía EW de aproximadamente 100 soldados que está capacitada para apoyar acciones locales dentro de unos 50 kilómetros utilizando sistemas más pequeños, como el R-330Zh Zhitel.

FIGURA: SISTEMA RB-341V LEER-3

Fuente: https://www.uasvision.com/

FIGURA: R-330ZH – ZHITEL



Fuente: https://www.armyrecognition.com/russia_russian_military_field_equipment/

Con esto vemos que la doctrina de EW rusa tiene en cuenta todas las operaciones.

El ejército ruso también cuenta con sofisticadas CCME, es decir, elementos para proteger sus sistemas de la EW del enemigo. Incluye tácticas y tecnologías para proteger sus propias transmisiones de radio para que no sean detectadas o bloqueadas. Las técnicas típicas incluyen las transmisiones en bandas de frecuencia angostas o transmisiones de baja potencia, así como formas de onda avanzadas que son resistentes a las interferencias, de forma similar a como lo hacen las fuerzas de la OTAN.

Sin embargo, sobre este último punto, algunos analistas afirman que no tienen suficientes equipos con estas características, con lo cual gran parte de las fuerzas operativas usarían equipos de comunicaciones de tecnología antigua.

Este último aspecto es considerado muy importante por muchos analistas, quienes destacan que se ha convertido nuevamente en quizás el aspecto más importante de EW, ya que Rusia y China implementan bloqueadores y sensores cada vez más sofisticados.

Al inicio de la invasión, muchos expertos vaticinaron que cuando las fuerzas rusas estuvieran listas para atacar, los sistemas terrestres y aéreos detectarían las emisiones radioeléctricas ucranianas y así sus fuerzas serían fácilmente atacadas con cohetes.

Sin embargo esto no se dio y las tropas ucranianas no perdieron el comando y control. Sin embargo, posteriormente cuando las tropas rusas se consolidaron en el este y en el sur, sí emplearon efectivamente los medios de EW. ¿Pero por qué no lo hicieron al inicio de la invasión? ¿Es esto razonable y coherente con el supuesto abandono del sistema Krasukha-4, mencionado anteriormente?

No podemos responder esto, nos falta información, y las acciones militares tienen objetivos, que a veces son tangibles, como la toma de un territorio, o la destrucción de activos. Otras veces esos objetivos no son explícitos, pueden ser hasta políticos y es difícil inferirlos.

Por otro lado, en las acciones al inicio de la guerra, el frente de avance ruso fue muy amplio y las acciones de guerra electrónica están, dependiendo de los objetivos y las frecuencias, condicionadas a las distancias. Esto justifica en parte su "fracaso" en algunas acciones, mientras que donde concentró poder la superioridad en el espectro se manifestó, y en ese caso, las acciones ucranianas, por ejemplo con drones se vieron limitadas o impedidas.

También hay que considerar el posible apoyo de Estados Unidos y la OTAN con inteligencia militar a las tropas ucranianas. Si bien la OTAN no interviene directamente en la guerra, si es parte del conflicto, y como aliados de Ucrania, pueden proporcionar valiosa información proveniente de satélites y otras fuentes, como lo hizo con el Reino Unido en la guerra de Malvinas.

Por el lado de Ucrania, en comunicaciones, recibieron radios modernas COMSEC (Seguras) con encriptación y salto de frecuencia, más otras CCME que hace que sobrevivan mejor en un ambiente EW hostil.

No sabemos sobre equipos de EW terrestres del lado ucraniano, se supone contarían con algunos equipos antiguos de origen ruso, y por parte de Occidente, si en drones y sistemas de defensa aérea como los Patriot suministrados por EEUU.

Superada la fase inicial de la guerra, ahora las tropas rusas se encuentran en el este, en territorio bajo su control, y pueden operar mejor los medios, con lo cual la EW surte efecto sobre las tropas ucranianas.

Con una mayor exposición a las radios suministradas por la OTAN, la EW rusa, pudo conocer un poco más sus características, y en consecuencia están comenzando a detectar y degradar las comunicaciones ucranianas. Las brigadas EW están utilizando los drones Orlan-10 de Leer-3 para detectar posiciones de artillería ucraniana en función de sus emisiones de radio, aunque el cifrado y el salto de frecuencia de las radios COMSEC las hace difíciles de interceptar y analizar. Como las líneas del frente ahora están mejor definidas en comparación con el inicio de las operaciones, las fuerzas rusas pueden asumir que las detecciones provienen de unidades militares ucranianas y actuar sobre ellos.

Se ha registrado que las brigadas EW rusas están utilizando el Krasukha-4 para bloquear los radares de drones ucranianos como el Bayraktar TB2 e interferir con sus enlaces de comunicación, protegiendo así los emplazamientos de artillería propia.

FIGURA: SISTEMA ORLAN 10

Fuente: Sputnik News

Los grupos tácticos de batallón (BTG) que operan en el sur y el este de Ucrania emplean sistemas de CME de VHF-UHF de menor alcance como el R-330Zh Zhitel para desactivar drones ucranianos que van desde Bayraktar TB2 hasta más pequeños como el DJI Mavics interfiriendo sus señales de GPS. Los BTG también están atacando las comunicaciones ucranianas utilizando bloqueadores R-934B VHF y SPR-2 VHF/UHF, con cierto éxito.

Por el lado de las fuerzas ucranianas, están aprovechando los sistemas EW suministrados por Estados Unidos y el entrenamiento para bloquear las comunicaciones rusas. También explotaron una debilidad de los grandes y poderosos sistemas EW rusos: son fáciles de detectar. Usando equipos EW suministrados por EEUU, las tropas ucranianas han podido detectar transmisiones de sistemas como Leer-3 o Krasukha-4 y realizar contraataques directos de cohetes, artillería y drones contra los sistemas rusos transportados por camiones.

Ucrania, por su parte ha buscado contar con más material EW barato para atacar las comunicaciones rusas, fundamentalmente empleando equipos basados en Software Defined Radio (SDR)[4]

La ciberguerra:

Mientras que la ciberguerra puede ocupar un lugar central durante la paz y en las acciones previas a la guerra, una vez iniciada la confrontación militar, la ciberguerra pasa a un papel auxiliar. La ciberguerra no puede ocupar territorio, ni puede matar y destruir a gran escala. Sus efectos son mucho menos predecibles que los de sus equivalentes físicos o convencionales. Incluso las victorias significativas suelen ser efímeras, transitorias y/o reversibles. También son inherentemente menos medibles y menos visibles que las victorias físicas y, por lo tanto, tienen mucho menos potencial para influenciar en la política interna del enemigo, a menos que estén consolidadas y cimentadas por victorias físicas en el terreno y sobre activos tangibles.

En consecuencia, los medios cibernéticos rara vez son las armas elegidas cuando las armas convencionales podrían emplearse de manera efectiva. Este punto de vista refleja y refuerza la creencia generalizada de que una vez que comienza la guerra, las armas cibernéticas quedan relegadas a un papel auxiliar.

Esto no minimiza la contribución potencial de la ciberguerra en el campo de batalla en este papel auxiliar. Las ciber-armas ofensivas pueden facilitar y complementar las operaciones convencionales causando diversos efectos adversos sobre el enemigo. Sin embargo, sí sugiere que, en el esquema más amplio de las cosas, los impactos cibernéticos quedan eclipsados por los de las operaciones convencionales y estos últimos siguen siendo la medida principal del éxito. Vemos que ha surgido un nuevo dominio de guerra significativo o una nueva capacidad. Este nuevo dominio o sistema de armas ha revolucionado la guerra probablemente.

Existe también y debemos considerar una relación importante entre la ciberguerra y la inteligencia. Así, la "inteligencia cibernética" es un componente destacado no solo de los esfuerzos de recopilación de inteligencia (y contrainteligencia), sino también de las operaciones encubiertas, las misiones de influencia y la guerra de la información.

En este caso, antes de la confrontación armada el creciente nivel de sofisticación de Ucrania en el dominio digital y la dependencia de los activos digitales han hecho que la inteligencia cibernética sea un factor constante en la confrontación de inteligencia entre Rusia y Ucrania. Pero Rusia no da tanta prioridad a este tipo de inteligencia, mientras que las capacidades de Ucrania se han visto reforzadas considerablemente por la asistencia masiva, a partir de 2021, de gobiernos y corporaciones occidentales.

4 https://www.fie.undef.edu.ar/ceptm/?p=11227

Las operaciones cibernéticas mantienen estrechos vínculos con la inteligencia, sobre todo cuando no hay en marcha ninguna operación militar a gran escala.

En el caso de Ucrania, la ciberguerra rusa, seguramente se apoyó mucho en la inteligencia, más teniendo en cuenta que Ucrania tenía estrechas relaciones con Rusia, y la posibilidad de contar con agentes que provean información sobre los sistemas informáticos y las redes. En este caso la inteligencia militar y/o nacional hace lo que se conoce en ciberdefensa como "ingeniería social". De esta forma cubre una parte elemental antes de las acciones, que es la reunión de información.

Desde el inicio del conflicto en 2014, Ucrania ha sufrido operaciones de inteligencia cibernética masivas y sostenidas e incluso ataques cibernéticos ejecutados por órganos estatales rusos y, a veces, aparentemente por terceros. Las operaciones fueron disruptivas e incluso destructivas contra la infraestructura crítica de Ucrania, como sus sistemas de generación y distribución de energía.

Sin embargo, en ese momento no se consideraba que cruzaran el umbral de la guerra, ni siquiera por parte de los adversarios occidentales de Rusia.

Existe un debate acerca de cuándo los ataques cibernéticos pueden ser considerados legítimamente actos de guerra. De hecho, las líneas entre las penetraciones legítimas e ilegítimas en tiempo de paz de las redes cibernéticas de los adversarios se han desdibujado y cuestionado constantemente, no solo por parte de China y Rusia, por mucho que la actividad de estas naciones parezca a veces particularmente imprudente.

Ni siquiera los debates en Naciones Unidas en el seno del UN – GGE /Group of Governmental Experts) han logrado consenso sobre este tema.

En el ámbito civil, como delitos informáticos, si se encuentran tipificados y las legislaciones avanzan cada vez más, pero no cuando hay naciones de por medio.

Los ataques fueron bastante fuertes sobre la infraestructura crítica de energía y comunicaciones, por ejemplo el ataque a los sistemas de Ukrtelecom.[5]

También sobre infraestructura de energía eléctrica como "blackEnergy" en 2015[6]. Incluso en 2022 dan cuenta de nuevos intentos, en este caso detectados y evitados por Ucrania.[7]

Las operaciones cibernéticas necesitan, como otras operaciones militares, una meticulosa planificación. Si bien no podemos citar una doctrina militar particular, sabemos que siguen algún proceso, que algunas empresas han modelado y publicado, como la Cyber Kill Chain de Lockheed Martin.

En general se parte de una reunión de información, definida por el objetivo a obtener.

Los elementos de ciberguerra deben crear una infraestructura clandestina para penetrar las redes adversarias, establecer un punto de apoyo secreto, reconocer toda la red y establecer un aparato de comando y control. La adecuada planificación es necesaria para convertir este punto de apoyo en un ataque concreto a los activos digitales del enemigo. En cualquier caso, la planificación debe desarrollar opciones completas para generar los impactos deseados, ya sea cuando se cumplan ciertos criterios o bajo demanda. En esta guerra, Rusia en la fase previa investigó y probó las capacidades de ciberdefensa de Ucrania.

El incentivo para lanzar ataques cibernéticos temprano, antes de que comience la confrontación convencional, se basa en dos consideraciones: apoyar las operaciones convencionales posteriores y hacerlo antes de que las acciones militares disminuyan la probabilidad de que los ataques cibernéticos planificados logren los efectos deseados. De hecho, como han observado algunos analistas, los

---

5 https://vpnoverview.com/news/ukraines-largest-telecom-company-hit-by-major-cyberattack/

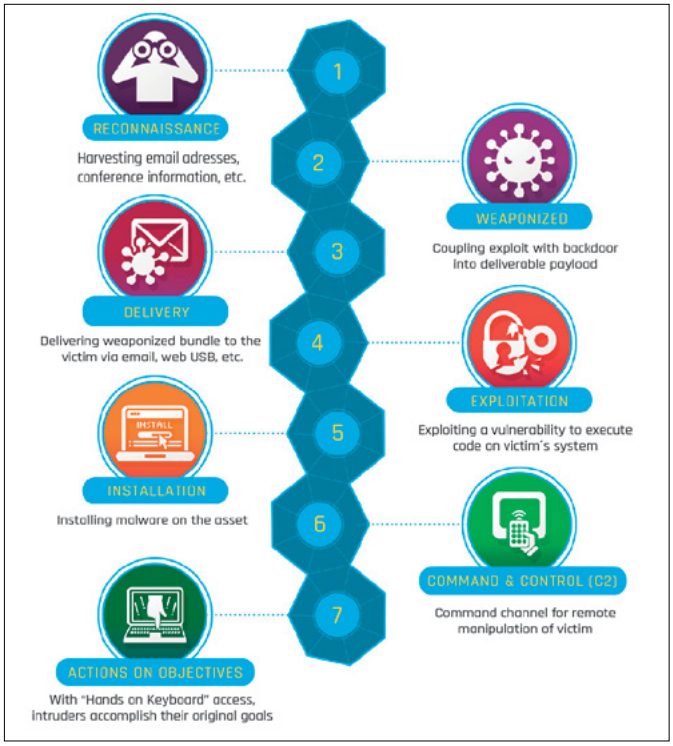
6 https://www.bbc.com/mundo/noticias-60850173#:~:text=En%202015%2C%20la%20red%20el%C3%A9ctrica,en%20el%20oeste%20de%20Ucrania.

7 https://www.swissinfo.ch/spa/afp/ucrania-frustra-un-ciberataque-ruso-a-sus-instalaciones-el%C3%A9ctricas/47514610

ataques cibernéticos rusos más importantes se llevaron a cabo muy temprano en el desarrollo del conflicto. Luego se desvanecieron en gran medida a partir del inicio de las operaciones convencionales, lo que sugiere que sus planificadores pueden haber buscado desencadenar sus ataques más sofisticados antes del ataque convencional. Sin embargo estos incentivos para atacar temprano implican costos políticos y operativos.

También podemos preguntarnos cuál fue el propósito de esos ataques cibernéticos previos al conflicto armado. Probablemente haya sido la disuasión. Mostrar que el acercamiento a Occidente tiene costos, por ejemplo.

FIGURA: "THE CYBER KILL CHAIN®"



Publicado por Lockheed Martin.

¿Cómo calcular los efectos de una acción cibernética? Según todos los informes, las operaciones cibernéticas durante este período ocasionalmente resultaron en daños colaterales significativos, especialmente en el lado ucraniano, pero en algunos casos también mucho más allá. NotPetya[8] se extendió a otros países y numerosas entidades civiles. Pero mientras que la conducta rusa en las fases más recientes de la guerra claramente buscó infligir el máximo daño colateral en Ucrania, sigue siendo incierto por ahora si el daño colateral infligido por las operaciones cibernéticas rusas antes de la guerra convencional fue intencional o no.

En el caso de Ucrania, preparó sus sistemas para minimizar la incidencia de los ataques, con el apoyo de entidades y empresas tecnológicas de Occidente, y se reflejó en el nivel de modernización, el empleo de sistemas en la nube, más robustos y distribuidos, las redes, el uso de starlink (servicio de internet de banda ancha, con el soporte de la constelación de satélites de SpaceX) y particularmente la "movilización" de un ejército TI (IT Army of Ukraine)[9]. Esto no busca la estruendosa caída de sistemas críticos, sino más actuar en el plano político y de la propaganda pero si induciendo a realizar algunos actos de hackeo como negación de servicio (DoS) y otros basados en scripts y programas para principiantes o aficionados que difunden.

En definitiva, estos grupos son numerosos, en su mayoría civiles, no pertenecen a organizaciones gubernamentales, y logran influir por medio de las redes sociales.[10]

8 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

9 https://twitter.com/itarmyukr?lang=en

10 https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities

Finalmente, como dijimos precedentemente, existen acciones "silenciosas" no percibidas que resultan extremadamente dañinas y contribuyen al éxito de las operaciones por parte del enemigo, especialmente de inteligencia. Tal es el caso descubierto recientemente del malware "snake", que se considera la herramienta de espionaje cibernético más sofisticada diseñada y utilizada por el Servicio Federal de Seguridad (FSB) de Rusia para la recopilación de inteligencia a largo plazo sobre objetivos sensibles. Existe una red a nivel global de máquinas infectadas que proporcionan información al FSB[11]. Esto fue descubierto por la America's Ciber Defense Agency.[12]

Conclusiones

La invasión de Ucrania muestra que EW sigue siendo importante y puede cambiar el curso de una guerra, como la conocida acción israelí en el Valle de Bekaa en 1982, durante la invasión israelí del Líbano en el conflicto con Siria. Sin el poderío aéreo o los drones guiados por satélite, las fuerzas de Rusia no podrían hacer funcionar bloqueadores o interferir más allá del horizonte para degradar las comunicaciones y los radares ucranianos antes de que las tropas avancen hacia Kiev. Obligadas a utilizar sistemas terrestres y aviones no tripulados de corto alcance, las brigadas rusas de EW que operaban con BTG (Grupos Tácticos de Batallón) tenían que preocuparse por no interferir con las operaciones amigas y no podían distinguir a las tropas ucranianas de los civiles. También tenían que mantenerse en movimiento, reduciendo la utilidad de sus grandes sistemas EW que por la potencia requerida no pueden operar en movimiento. Pero Rusia está superando esos problemas ahora porque el aparente objetivo de tomar rápidamente Kiev fracasó y se convirtió en una guerra de desgaste en el sur de Ucrania con posiciones mejor definidas.

Sin embargo, el problema de la superioridad aérea parece persistir porque Ucrania tenía y fue reforzado por Occidente con diversos sistemas de defensa aérea. Entonces, por el momento, incapaces de superar el horizonte, las unidades terrestres EW rusas pueden bloquear o interferir a las tropas ucranianas solo cuando están separadas por líneas de batalla claramente definidas. Se basan en sistemas como Leer-3 para encontrar las emisiones ucranianas para que la artillería rusa pueda atacar a los ucranianos con proyectiles y cohetes. Los sistemas EW rusos como Krasukha-4 y R-330Zh Zhitel pueden desactivar el GPS o los radares en los drones ucranianos, pero no es sustancialmente diferente de derribar aviones con armas. Y aunque los sistemas como el Moskva-4 podrían escuchar señales en el horizonte, Rusia parece no aprovechar demasiado esas detecciones, tal vez por prudencia, al no poder corroborar esa información por otros medios y así evitar el derroche de munición y los daños colaterales a civiles.

Quizás la mayor lección de Ucrania para EW es que ganar la radiofrecuencia no es igual a ganar la guerra. Rusia está en el dominio de la guerra EW en este momento. La situación podría cambiar rápidamente si las tropas de Ucrania, con el apoyo occidental, recuperan el control aéreo de Ucrania, en los sectores ocupados por Rusia, donde podrían actuar contra el enemigo.

Para ambos bandos, el desafío para dominar el espectro electromagnético es contar con medios y personal capacitado, pero también hay que tener en cuenta que la EW se desarrolla en el espectro electromagnético, que depende de las leyes de la física. Por lo tanto las fuerzas militares deberán adecuar sus movimientos para cumplir esas leyes y ser efectivos en el despliegue táctico y en sus distancias.

En cuanto a las operaciones de ciberguerra, es más difícil medir sus efectos cuando el conflicto armado está en desarrollo. Es muy probable que lo actuado previamente de sus frutos si el trabajo

11 https://www.fie.undef.edu.ar/ceptm/?p=12262

12 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

fue bien realizado, particularmente como medio de reunión de información de inteligencia. Esto puede ser más perjudicial que las acciones contundentes sobre sistemas que se inutilizan, y se hacen visibles las acciones. A veces, entonces como un iceberg, lo que no se ve puede ser más peligroso y perjudicial, por cuanto el enemigo podría tener una fuente de reunión de información en la red sin despertar sospechas.

Sin duda, en la etapa previa al conflicto armado, hubo como dijimos acciones contundentes que hicieron efecto sobre la infraestructura de Ucrania, e incluso otros países incluido EEUU, como el ataque al Colonial Pipeline, que si bien hubo acusaciones contra Rusia, nunca lo reconocieron, como es usual en este tipo de acciones. Como sea, nunca conoceremos en lo inmediato los objetivos reales como para evaluar tan pronto sus resultados.

La Guerra Electrónica ya había ganado un lugar como multiplicador de fuerza, y la ciberguerra, sin duda también ya lo ha hecho, con consecuencias que se sienten mucho más fuera del campo de combate, en tanto somos cada vez más dependientes de las TICs.

Fuentes

i. RUSI (Royal United Services Institute for Defence and Security Studies)
ii. Ukraine at War - Paving the Road from Survival to Victory - Jack Watling and Nick Reynolds
iii. IEEE Spectrum, julio de 2022 - “La caída y el auge de la guerra electrónica rusa “.
iv. Carnegie Endowment - Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict - Ariel (Eli) Levite.
v. CSIS (Center for Strategic and International Studies) - Evolving Cyber Operations and Capabilities – Mayo 2023.

(*) 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