AÑO III - N 4
2025
URUGUAY

Revista ECEME

Nivel Estratégico

Democratización del Poder Aéreo

Investigación

Análisis Prospectivo en la Educación Militar
Trabajos de Investigación Militar

Nivel Operacional

Conflicto armado Rusia-Ucrania

Historia

General de División Don Pedro Sicco

REVISTA DIGITAL
Escuela de Comando y Estado Mayor del Ejército

Escuela de Comando y Estado Mayor del Ejército

Revista ECEME

(REVISTA DIGITAL)

AÑO III - NÚMERO 4

2025

Foto de tapa: Clausura de Cursos del I.M.E.S. 2024. Dpto. Com. Inst. del Ejército.

ÍNDICE

Escuela de Comando y Estado Mayor del Ejército

FINALIDAD

- Capacitar a los Señores Jefes integrantes del Cuerpo de Comando, Cuerpo de Apoyo y Complemento, y el Cuerpo de Servicios, para desempeñarse en la jerarquía de Jefe, como integrante de los distintos Escalones Tácticos y Administrativos en tiempo de paz, crisis o conflicto armado.
- Formar Oficiales de Estado Mayor para actuar en tiempo de paz, crisis o conflictos armados como asesores de los distintos Comandos Estratégicos, Tácticos y Administrativos.
- Iniciar a los Jefes Alumnos en el estudio de los problemas de Seguridad y Defensa, con énfasis en la planificación estratégica de estructuras orgánicas, administrativas y operativas.

MISIÓN

- La Escuela de Comando y Estado Mayor del Ejército (E.C.E.M.E.) tiene por misión desarrollar los Cursos de Estado Mayor, de Capacitación y Perfeccionamiento de Jefes y Preparatorio de Comando y Estado Mayor.
- Capacitar a los Mayores Combatientes y de los Servicios Generales para desempeñarse en la jerarquía de Jefe, como integrantes de los distintos escalones tácticos y administrativos, en tiempo de paz o en el marco de las operaciones previstas para atender las hipótesis vigentes de conflictos armados.
- Formar Oficiales de Estado Mayor como asesores de los distintos Comandos Estratégicos, Tácticos y Administrativos en el marco de la doctrina vigente.
- Asesorar sobre las medidas conducentes a la elevación del nivel de conocimientos científicos - tecnológicos, necesarios a los integrantes de la Fuerza.
- Elevar el conocimiento profesional de los Capitanes.

VISIÓN

- Continuar siendo el órgano esencial del Instituto Militar de Estudios Superiores, manteniendo un elevado nivel de capacitación de los Oficiales Jefes del Ejército Nacional para proporcionarles los conocimientos superiores necesarios, en lo relativo al Comando de los distintos Escalones Tácticos y Administrativos y al Estado Mayor desde el nivel Táctico terrestre al más alto nivel Estratégico Conjunto/Combinado.
- Constituirse en el Centro de Enseñanza de nivel Universitario con mayor prestigio y solidez del Sistema Educativo Militar, reconocido y valorado nacional e internacionalmente por la calidad educativa de sus procesos de perfeccionamiento, formando líderes integrales, innovadores, generadores de conocimiento y pensamiento estratégico, en Seguridad y Defensa Nacionales, con el propósito de contribuir al desarrollo del Estado y afrontar los escenarios cambiantes del futuro.

Revista ECEME

PALABRAS DE LA DIRECTORA DE LA E.C.E.M.E.

CORONEL ANDREA DE LOS SANTOS

Oficial Superior del Arma de Infantería, actualmente desempeña funciones como Directora de la Escuela de Comando y Estado Mayor del Ejército.

Prestó servicio en diferentes unidades del Arma y en la Escuela Militar como Instructora.

Es Diplomada en Estado Mayor y Licenciada en Ciencias Militares.

Estimados lectores de la revista E.C.E.M.E., es un honor dirigirme por primera vez como Directora de la Escuela de Comando y Estado Mayor del Ejército, Institución que, desde su creación, ha sido sinónimo de rigor académico, profesionalismo y compromiso con la excelencia. Asumo esta función con un profundo sentido de responsabilidad, consciente del legado recibido y del desafío que implica conducir la formación de quienes serán los futuros asesores y comandantes de nuestra Fuerza.

Nuestra Escuela se encuentra hoy en una etapa clave, marcada por la consolidación del Sistema de Educación Militar y con ello, por el fortalecimiento de la Maestría en Estrategia Militar Terrestre. En un mundo caracterizado por su complejidad, incertidumbre y permanente transformación, adquiere mayor relevancia el pensamiento crítico, la capacidad de adaptación y el pensamiento estratégico. En este contexto, la E.C.E.M.E. reafirma su misión de formar Señores Oficiales Jefes capaces de asumir funciones de media y alta dirección, incentivando el espíritu crítico e innovador y capaces de analizar problemas de Seguridad y Defensa en escenarios operativos, estratégicos y multidimensionales.

Las páginas de esta Revista reflejan fielmente ese compromiso Institucional. Cada artículo, elaborado por nuestros exalumnos y alumnos actuales de la E.C.E.M.E., constituye un aporte al estudio y al debate de los desafíos contemporáneos en los ámbitos estratégico, operacional y táctico. Esta publicación se ha consolidado como un espacio para la difusión del conocimiento militar, y como una herramienta académica que proyecta el trabajo cotidiano de nuestras aulas hacia el Ejército Nacional, las Fuerzas Armadas y la sociedad en su conjunto.

A todos quienes han contribuido en esta edición (autores, instructores, editores y alumnos) les expreso mi reconocimiento y felicitaciones. Los invito a continuar escribiendo, investigando y generando nuevo conocimiento, guiados por la vocación de servicio, el rigor profesional y el espíritu de superación permanente que distinguen a nuestra profesión militar.

Finalmente, que esta nueva edición de la Revista E.C.E.M.E. inspire en todos nuestros Jefes alumnos el estudio, el análisis profundo y la búsqueda permanente de la excelencia, pilares para el desarrollo profesional individual y para el fortalecimiento de nuestro Ejército Nacional.

"TANTO MARTE COMO MINERVA"

En la mitología clásica, Minerva y Marte representan dos aspectos fundamentales en la formación de los Oficiales de Estado Mayor: la sabiduría y la estrategia por un lado, y la valentía y el coraje por el otro.

Minerva, diosa de la sabiduría, simboliza la necesidad de un conocimiento profundo, la reflexión estratégica y la capacidad de tomar decisiones informadas.

Marte, dios de la guerra, encarna el valor, la disciplina y la fortaleza necesarios en el campo de batalla.

Los alumnos de la Escuela de Comando y Estado Mayor del Ejército deben, por tanto, integrar estas dos virtudes en su formación.

Como Minerva, deben cultivar la inteligencia, la previsión y la comprensión de los complejos escenarios geopolíticos y tácticos.

Como Marte, deben estar preparados para actuar con decisión y coraje, liderando con firmeza en la defensa de la Patria.

Esta dualidad, donde la sabiduría guía la acción y la acción se enmarca en la sabiduría, es lo que define a un verdadero líder militar.

En cada decisión, en cada estrategia, el equilibrio entre Minerva y Marte asegura que las acciones en el campo de batalla no solo sean valientes, sino también prudentes y efectivas.

Así, los futuros líderes formados en esta Escuela están llamados a ser tanto sabios como guerreros, maestros en el arte de la guerra y guardianes del bienestar Nacional.

Mayor Andrés Amil
Mayor Gonzalo Madeiro
Mayor Pablo Torello
Mayor José E. Ferreira
Mayor Walter Barreiro
Mayor Alejandro Volpe

Marca de agua:
Representación de Marte y Minerva, de la mitología Romana.
Fuente: https://enciclopedia.net

Revista ECEME

Edición y publicación de índole académica, de acceso abierto, orientada a visibilizar los resultados del estudio y la investigación de las ciencias militares.

VALORES

- Integridad Académica
- Colaboración Multidisciplinaria
- Innovación en Educación Militar
- Formación Crítica y Reflexiva
- Accesibilidad y difusión

MISIÓN

Difundir contenidos de calidad producidos en el aula de los cursos de la ECEME, que contribuyan a incentivar la investigación, la publicación de resultados y la difusión de conocimiento en el campo de las ciencias militares.

VISIÓN

Constituirse en una publicación de referencia para las FF.AA., a partir de un proceso editorial preciso, confiable, relevante y compendiado en forma atractiva.
Erigirse en un elemento didáctico para todo miembro de la comunidad educativa del I.M.E.S., como centro de Postgrado del Ejército Nacional.

OBJETIVO

Contribuir a la difusión del conocimiento de las ciencias militares, mediante una publicación periódica en línea, multidisciplinaria y de acceso abierto, orientada a hacer visibles algunas de las tareas asignadas por el Cuerpo Docente a los alumnos de la E.C.E.M.E.

Acercar a los actuales y futuros alumnos de la E.C.E.M.E. a los contenidos de las materias y unidades temáticas que estudian, de un modo más profundo y reflexivo.

ESTRATEGIAS

- Constituir un órgano de difusión de trabajos de investigación parciales o definitivos. Su naturaleza es multidisciplinaria, por ello sus dos números anuales se estructuran en los siguientes campos: Estrategia, Táctica, Ingeniería Militar, Investigación y Administración Militar.
- Despertar interés por la creación de nuevos contenidos, desde una actitud positiva, motivada y curiosa hacia el aprendizaje.
- Realizar un proceso crítico de la información y las fuentes, así como la búsqueda y tratamiento de las mismas.
- Habituar a los alumnos a producir, revisar y editar los documentos de tipo académico-científicos, contribuyendo al entrenamiento hacia el trabajo final de grado o de magister.
- Habilitar al alumno a desempeñar el rol de difusor del conocimiento

LA DEMOCRATIZACIÓN DEL PODER AÉREO: Análisis del Impacto Estratégico Militar de los Sistemas Aéreos no Tripulados de Bajo Costo en la Guerra Moderna.

IMAGEN: Soldado del Ejército Nacional operando un dron en Op. Frontera Segura
FUENTE: Departamento de Comunicación Institucional del Ejército

Revista ECEME

MAYOR JOSÉ MACHADO

Oficial Jefe del Arma de Infantería, actualmente Jefe de las Divisiones II y III de la D.E.IV.

Es Diplomado en Estado Mayor y Magister en Estrategia Militares Terrestre

Prestó servicios en diferentes Unidades del Arma.

Participó en M.O.P. en la República de Haití en 2011.

PALABRAS CLAVES

ESTRATÉGIA
DRONES
INTELIGENCIA ARTIFICIAL

INTRODUCCIÓN:

En cumplimiento con los objetivos académicos del Curso de Estado Mayor 2024, dentro del marco de la asignatura Estrategia II, el presente artículo analiza las oportunidades que ofrece el empleo de ésta tecnología barata y de fácil acceso frente a los desafíos que implica enfrentarla en condiciones de inferioridad o habiendo negado sus ventajas.

Los drones de ataque pequeños y de bajo costo representan una capacidad de combate novedosa y asimétrica. Estos sistemas aéreos no tripulados (UAS, por sus siglas en inglés) se caracterizan por su tamaño diminuto y su costo de producción relativamente bajo, lo que facilita el despliegue masivo y la flexibilidad operativa. A diferencia de los drones militares más grandes y sofisticados, su simplicidad permite una rápida proliferación y facilidad de uso, incluso por actores no estatales.

Si bien carecen de los sensores y las capacidades de cargas útiles de los UAS de mayor porte, estos drones aprovechan eficazmente tecnologías económicas y disponibles comercialmente para fines letales. Su pequeño tamaño hace que sea difícil detectarlos y rastrearlos con los sistemas de defensa aérea tradicionales, mientras que su bajo costo permite un alto grado de desgaste.

Su adaptabilidad y facilidad de modificación representan un desafío persistente y en evolución para las fuerzas militares convencionales y para los cuerpos policiales, y de seguridad pública y privada en general.

EVOLUCIÓN DE LOS DRONES PEQUEÑOS DE ATAQUE:

La evolución de los sistemas aéreos no tripulados de ataque, pequeños y de bajo costo puede caracterizarse por fases superpuestas que han transformado rápidamente el campo de batalla.

La fase inicial es previa al 2010, se dio con la maduración de la tecnología de

cuadricópteros comerciales, estableciendo la plataforma fundamental para la subsiguiente militarización. Esta base accesible y rentable facilitó las primeras adaptaciones militares, centradas principalmente en la integración básica de cargas útiles.

La fase siguiente fue la integración de dispositivos explosivos improvisados (IED por sus siglas en inglés), este periodo abarca de 2010 a 2015 aproximadamente. Este período fue testigo de una adaptación generalizada de UAS comerciales para uso militar y paramilitar. La proliferación de información de código abierto y componentes fácilmente disponibles permitió la integración de IED cada vez más sofisticados.

La siguiente fase incorpora sistemas diseñados específicamente para ataque, ya que la industria militar se incorpora a la carrera armamentística en éste campo, antes dominado por lo artesanal y amateur.

Estos sistemas incorporan características avanzadas como mayor alcance, mayor capacidad de carga útil y contramedidas electrónicas mejoradas.

Para ello emplean impresoras 3D y materiales adquiridos en venta libre por e-commerce, realizando el armado a mano en edificios particulares, lo que dificulta[1] enormemente su detección y sabotaje por parte del bando contrario.

Asimismo como etapa de ésta fase, se encuentra el empleo de fibra óptica para el guiado de los aparatos, de ésta manera se anula el efecto de la guerra electrónica enemiga y se obtiene una mejor calidad de imagen y estabilidad en la señal. La limitante está dada por el alcance y resistencia de los cables, pero pueden alcanzar fácilmente los 10 kilómetros y las nuevas adaptaciones han duplicado ésa distancia, esto tanto partiendo desde la posición del piloto, como estar conectados a un receptor y permitir que el operario aún se encuentre posicionado más lejos.

La etapa más reciente, iniciada hace relativamente poco tiempo, son las operaciones de enjambre y la integración de inteligencia artificial (IA), es parte del presente y parece ser el futuro del empleo de ésta tecnología.

Esto permite ataques coordinados complejos que pueden abrumar los sistemas de defensa tradicionales, actualmente los enjambres son pequeños y tienen cada aparato a un piloto, guiados y coordinados por un dron de observación, éste marca el blanco a atacar y los pilotos realizan secuencias de padrones de vuelo y ataque sucesivos o simultáneos sobre un mismo blanco, saturándolo e impidiendo una reacción efectiva al ataque.

Pero con la integración de IA ya se emplea "dron nodriza" con un solo operario, el cual tiene a varios drones volando cerca en forma autónoma, estos se lanzan sobre los objetivos que le marca el operario del dron nodriza, empleando IA para reconocer el blanco y seleccionar el mejor modo de acercamiento y ataque. Asimismo con esta base se puede transportar a drones de menor porte y alcance, para aumentar su rango de acción, actuando a su vez, la nodriza, de repetidor de señal.

Los drones nodrizas pueden ser aéreos, terrestres o navales, siendo los más efectivos, actualmente, el primero y el último. Éste método permite alcanzar[2] blancos incluso a cientos de kilómetros del operario, como es el caso de un reciente ataque que empleó un dron naval para acercar un dron aéreo a la costa de Crimea, controlada por Rusia, atacando infraestructura energética en el mar.

Esta evolución demuestra una tendencia acelerada hacia drones de ataque de bajo costo, cada vez más letales y energéticamente eficientes. La rapidez de este avance tecnológico continúa superando el desarrollo de contramedidas efectivas, planteando desafíos significativos para la defensa y la estrategia militar tradicional, esta democratización de la potencia aérea está redefiniendo los equilibrios de poder en conflictos tanto simétricos como asimétricos.

En conclusión, la evolución de los sistemas aéreos no tripulados de ataque, de pequeño porte y de bajo costo, no solo ha transformado las tácticas militares en vigencia, sino que también ha alterado principalmente la dinámica de los conflictos a nivel estratégico. A continuación se analizará y fundamentará ésta

1 Al decir uso militar se refiere al empleo por parte de ejércitos regulares. Uso paramilitar refiere a grupos de milicias, insurgentes, criminales, terroristas, etc.
2 También llamados "manadas", por ser integrados de pocos aparatos, considerándose que aún no llegan al nivel de "enjambre".

afirmación empleando los factores del Potencial Nacional. (Amado et al., 1980)

ANÁLISIS DE LA SITUACIÓN.

Impacto en el Factor Militar.

Éste es el factor más afectado, a criterio de éste autor, puesto que el empleo de ésta tecnología en desarrollo, ya ha obligado a un cambio en la configuración del Campo de Batalla. La profundidad y frente de influencia de una fracción tan pequeña como la Sección de Fusileros, alcanza niveles antes conferidos a una División. El hecho de que un Soldado a órdenes de un Teniente, tenga la capacidad bombardear un Punto de Colección de Material de Brigada o de División, o destruir un Radar de Defensa Antiaérea de Largo Alcance, obliga a tomar medidas extremas de seguridad, modificando el ritmo de las operaciones, lo rápido ahora es lento y viceversa.

Se ha transparentado el Campo de Batalla por la presencia de un cúmulo de sensores remotos en todos los escalones de comando, accionando en frente y profundidad, lo que asimismo complejiza el proceso de toma de decisiones de los propios usuarios, que pueden ver afectadas negativamente sus acciones por la presencia o el accionar de sUAS de unidades adyacentes, de la retaguardia o incluso de aquellas que operan infiltradas en la retaguardia enemiga o que sirven a niveles estratégicos, como los drones de largo alcance que efectúan reconocimiento y adquisición de blancos para misiles.

Este Campo de Batalla Transparente, obliga a un cambio drástico tanto en las operaciones de Defensa como de Ofensiva, estos cambios comienzan a nivel técnico y táctico, pero escalan a los demás niveles. Esto se debe a que los planes a nivel Estratégico y Operacional requieren de coordinaciones que afectan transversalmente a todos o casi todos los elementos de que componen a los Estados (dependiendo de la dimensión y complejidad del mismo) y que aportan directa o indirectamente al esfuerzo militar, pero en última instancia, el éxito del plan se basa en el grado de éxito de las operaciones ejecutadas por pequeñas unidades de nivel Batallón o Compañía, escuadrillas de la Fuerza Aérea o Buques de la Armada.

Si estos se enfrentan a amenazas inesperadas o para las que no tienen contramedidas (cómo los drones navales y los aéreos FPV o de bombardeo), su eficiencia se verá reducida o anulada, por lo que mantendrá la situación táctica congelada, obligando a los contendientes a encarar un enfrentamiento de desgaste, que ganará el que tenga la capacidad de asumir más pérdidas y seguir operativo, o de generar una Capacidad que le devuelva la iniciativa. Pero por el momento todas las contramedidas ensayadas y aplicadas han sido insuficientes para frenar ésta amenaza.

La situación descripta no solo se aplica a la Guerra Convencional y a gran escala, puede suceder en una Guerra Irregular y asimétrica o en el enfrentamiento de Fuerzas de Seguridad contra el Crimen Organizado, o en una guerra entre organizaciones criminales, cómo es el caso de las disputas entre Cárteles en México.

En lo que a operaciones ofensivas se refiere, el empleo de drones en Ucrania ha afectado la movilidad de las fuerzas terrestres, navales y aéreas, pero en lo que al Componente Terrestre de una operación refiere, éste vehículo aéreo armado tiene la capacidad de causar baja en todos los elementos presentes en el Campo de Batalla Terrestre actual. Desde el soldado conscripto hasta el Tanque Principal de Batalla mejor protegido y equipado con los mejores sensores y defensas activas y pasivas, obligando a la modificación de los vehículos por parte de sus usuarios hasta dejarlos irreconocibles, sacrificando

Imagen: Modificación improvisada de un T-80BVM en un "Tanque Tortuga".
Fuente: https://es.topwar.ru/246877-v-avangarde-nastupajuschej-rossijskoj-morskoj-pehoty-prodvigaetsja-tank-cherepaha.html

todas las cualidades en favor de la protección, para aumentar la capacidad de supervivencia. Éste concepto ha permeado incluso a la Industria Militar, que ya ha tomado buena nota de las lecciones aprendidas con sangre en el terreno y comienza a industrializar estos diseños de oportunidad.

Estos mismos drones de ataque realizan reconocimiento al mismo tiempo que buscan un blanco, aunque cuenten con la asistencia de aparatos de observación que los supervisan y guían. El volar más cerca del suelo les permite identificar objetivos que pueden estar mejor camuflados para la vista aérea. Actualmente están siendo dotados con IA, que facilita la identificación de blancos, brindando actualizaciones de información en tiempo real a una velocidad que excede las capacidades humanas de observación y procesamiento de información.

El dron de pequeño porte se ha convertido en una plataforma multi rol, capaz de ser útil para la tropa de infantería en roles de observación, ataque, oscurecimiento, iluminación de blancos e incluso contra otros drones. Para la tropa blindada ha servido, entre otras cosas, para sustituir a un observador avanzado, permitiendo realizar fuego indirecto con Tanques a distancias que superan la capacidad de las ópticas del vehículo pero que están dentro del alcance máximo del arma principal. Para la tropa de ingenieros ha permitido sembrar minas, moverlas de lugar, plantar minas nuevas, realizar destrucciones de puentes sin emplear un elemento de zapadores humano en el lugar, incluso activar las voladuras preparadas pero no ejecutadas por los ingenieros enemigos. Para la artillería han permitido realizar fuego preciso en la profundidad de la retaguardia enemiga, sin emplear observadores infiltrados en la retaguardia y relativizando la importancia de dominar las alturas del campo de batalla, que si bien persiste, ya no es una condición indispensable para tener dominancia en la observación. Esto ha generado que el arma más letal de la Guerra en Ucrania fuera la Artillería hasta mediados de 2024, cuando la balanza parece haberse inclinado en favor de los drones; se ha estimado por estudios recientes que hasta el 75% de las bajas de personal y el 65% de las bajas de blindados confirmadas visualmente, son producto de la acción de éstos aparatos. (Amran, 2024)

Ésta capacidad de verlo todo, todo el tiempo, ha generado que concentrar tropas para el lanzamiento de un ataque se vuelva una acción suicida, por lo que las tropas se dispersan y enmascaran para luego concentrarse en el último momento e incluso sobre la marcha para lanzar el ataque, con una fuerza muy limitada, normalmente de nivel Sub-Unidad, enfocando el esfuerzo en un solo eje y en un punto muy limitado del frente, para luego ser reemplazada o reforzada con elementos de similar valor, siendo actualmente escasos los ejemplos de ataques superiores al de nivel Unidad en forma simultánea. Obligando a los asaltantes a maximizar el empleo de operaciones de engaño y los movimientos de aproximación subterráneos para lograr ataques eficaces y con un costo relativamente bajo. El ejemplo más reciente de esto es la ofensiva rusa en Kursk en marzo de 2025, empleando un gasoducto en desuso.

Esta incapacidad de enmascarar eficientemente movimientos de grupos superiores a la Sección, se traslada a las operaciones de Defensa, que han visto su nuevo apogeo en la Guerra de Ucrania, que ha visto renacer el concepto de línea de defensa continua y estática, basada en Puntos Fuertes interconectados por líneas de trincheras en frente y profundidad, apoyándose en obstáculos del terreno y artificiales como zanjas anti tanque, líneas de dientes de dragón y densos campos minados. Pero ejemplos de posiciones de combate basadas en atrincheramientos no solo se dan en Ucrania y Rusia, se pueden encontrar en México empleados por los Cárteles para defender sus territorios de otros grupos delictivos y de las Fuerzas de Seguridad gubernamentales, o también en conflictos que se desarrollan en el Congo, en Myanmar y Nagorno-Karabaj, entre otros ejemplos.

Si bien protegerse detrás de obras defensivas ha dado buenos resultados desde que la humanidad abandonó la vida nómade, nunca antes, hasta ahora, el humano ha tenido tantos medios distintos para observar desde el cielo y/o a través de las barreras defensivas, medios que van desde cámaras comunes montadas en drones, sensores de radares de vigilancia terrestre y satélites militares y civiles que fácilmente pueden proveer de información en tiempo real a quien cuente con los recursos necesarios

para acceder a ellos.

Esto dificulta en extremo la capacidad de construir posiciones defensivas sin ser visto y mapeado en tiempo real por el enemigo, o incluso por civiles entusiastas que siguen los conflictos en tiempo real, publicando contenido en internet. Lo cual permite que el atacante interfiera con las obras de preparación del terreno a través del ataque con drones de bombardeo o kamikaze, o con otros medos de fuego indirecto disponibles.

Sin embargo el dron representa un elemento sumamente apto para la defensa, permite a los escalones inferiores de la Unidad que ocupa una determinada posición, tener un conocimiento en tiempo real de la situación, a través de la detección de movimientos y de concentraciones de medios y de tropas enemigas, que antes fácilmente se podían ocultar de la observación y del fuego directo en zonas muertas del campo de observación y tiro, en la oscuridad, la niebla o de pantallas de humo, incluso a más de diez kilómetros de distancia. Esto, como se expresó anteriormente, vuelve imposible concentrar tropas de nivel superior a los veinte hombres y más de tres o cuatro vehículos blindados y/o tanques, sin llamar la atención y convertirse en un blanco valioso para la artillería, morteros y aviación de ala fija o rotatoria, aunque actualmente es muy probable que el primer agresor sea un operador de dron que sirva a la fracción que realizó la detección, actuando en conjunto con el operador del aparato de observación. Asimismo pone casi en obsolescencia la planificación de "blancos revelados" por parte de la artillería de campaña y su posterior batida con fuegos a horarios, redundando en una economía de tiempo y de medios.

La capacidad de detectar movimientos enemigos en forma tan temprana, como sucedió en la conducción de la defensa de la "Linea Surovikin" por parte de las tropas rusas, permite al defensor aplicar un abanico de respuestas, únicas, simultaneas o sucesivas, limitando en gran medida las reacciones del atacante o permitiéndole predecirlas también, posibilitando la preparación de una contra reacción con mucho tiempo de antelación.

Esta intromisión no buscada de los escalones más bajos en el ciclo OODA[3] de los escalones más altos (incluso de nivel Operacional), mal gestionado y sin un cambio de paradigma en la estructura jerárquica y de pensamiento (que por norma general es vertical, formal y estructurada) de las organizaciones militares, sin lugar a dudas generará conflicto, desaprovechamiento de los recursos, desconfianza y un exceso de aplicación de medidas de control, lo cual conllevará a la perdida en la iniciativa y la pro actividad del mando a nivel táctico y por consiguiente, será pasible de quedar en inferioridad ante enemigos que independientemente de sus recursos materiales y humanos, puedan aplicar un ciclo de toma de decisiones más rápido y con mayor libertad para los escalones más bajos.

En resumen, gracias a los UAS de pequeño porte y bajo costo, el campo de acción e influencia de los escalones inferiores en las organizaciones militares y paramilitares se ha visto aumentado exponencialmente en un corto periodo de tiempo, convirtiendo a los jóvenes oficiales, sargentos y cabos en agentes con capacidad de incidir en el nivel Operacional e incluso Estratégico del Campo de Batalla, adquiriendo éstos un protagonismo y relevancia propio del que pueden alcanzar "Caudillos" en ambientes de Teatros de Guerra Irregular o de conflictos de bandas criminales. Todo lo cual fuerza al incremento de las medidas de selección y posterior especialización de estos cuadros, con vistas a mejorar su integración dentro del mosaico que compone la tendencia actual de los conflictos "Multidominio". (Pulido, 2021)

CONCLUSIONES.

Desde una perspectiva filosófica de la Guerra, en lo que refiere a la dialéctica bélica, la irrupción de los sistemas aéreos no tripulados de bajo costo representa una inflexión ontológica, una redefinición fundamental del poder aéreo y su proyección estratégica. Se puede observar cómo esta tecnología, otrora circunscrita a las grandes potencias, se ha democratizado, otorgando capacidades asimétricas a una multiplicidad de actores, estatales y no estatales por igual.

Desde una perspectiva militar, se percibe una erosión de las jerarquías tradicionales del campo de batalla. La Sección de Fusileros, ahora investida con la capacidad de

[3] El acrónimo representa las cuatro etapas del modelo mental de toma de decisiones que fue desarrollado por el Coronel John Boyd: Observar, Orientar, Decidir, Actuar.

proyección ofensiva a Nivel Operacional, desafía la doctrina clásica y exige una reevaluación de las tácticas y probablemente de las estrategias tradicionales. La transparencia total del Campo de Batalla, resultado de la vasta red de sensores presentes en todos los dominios, obliga a la dispersión y el enmascaramiento de las fuerzas militares por pequeñas que sean, mientras la defensa estática experimenta un renacimiento paradójico ante las amenazas casi omnipresentes en todos los espectros y campos.

Reflexionando de manera prospectiva, la trayectoria evolutiva de estos sistemas apunta hacia la autonomía y la inteligencia artificial, anticipando un futuro donde los enjambres de drones autónomos podrían dominar el espectro aéreo, lo mismo que sus homólogos de tierra y agua, dentro de sus ámbitos. La carrera armamentística se desplaza hacia la contienda algorítmica y la guerra electrónica, donde la capacidad de adaptación y la innovación tecnológica serán los factores determinantes de la superioridad y la obtención y retención de la iniciativa durante las Campañas bélicas.

La democratización del poder aéreo mediante los sistemas aéreos no tripulados de bajo costo no es meramente una innovación Táctica, sino una transformación Estratégica Militar de profundas implicaciones filosóficas, políticas, económicas y técnicas. Es previsible que obligará a una reevaluación constante de las doctrinas, a una adaptación ágil de las defensas y a una reflexión profunda sobre las implicaciones éticas y sociales de esta nueva concepción de la guerra, con su respectiva revisión normativa de índole Nacional como Internacional.

La comprensión y el dominio de esta tecnología serán determinantes para garantizar la supervivencia de las tropas, el cumplimiento de las misiones fundamentales de las Fuerzas Armadas en cuanto a mantenimiento de la soberanía, control del territorio por parte del Estado y su proyección de poder y disuasión en el futuro cercano.

Referencias Bibliográficas

Amado, F. D., Pomoli, J. J., & Torello, H. C. (1980). *Estrategia. Apuntes, Enfoques, Proposiciones.* (Vol. N° 60).

Amran, R. (9 de abril de 2024). *OTAN: Los drones ucranianos son responsables de más del 65% de los tanques rusos destruidos*. The Kyiv Independent,

Averchuk, R. (19 de setiembre de 2024). *Drones rusos a la caza de los civiles*. Swissinfo.ch.

Cole, B. (20 de agosto de 2023). *Seis aviones rusos Il-76 y un bombardero Tu-22 fueron alcanzados en un ataque nocturno con drones en Pskov*. Newsweek

Defense Express. (3 de agosto de 2023). Defense Express.

Espino, M. (20 de marzo de 2025). *Juez ordena al gobierno Federal y de Michoacán evitar desplazamiento forzado*; *da 48 horas para eliminar explosivos caseros del narco*. El Universal.

Goncharova, O. (9 de febrero de 2025). *Ukraine to launch 'Drone Line' project to enhance battlefield operations*. The Kyiv Independent.

Hercules, (s.f.) La importancia de los drones en la guerra de ucrania

Hernando, P. (19 de marzo de 2025). *Elon Musk: "Hay un 20% de posibilidades de que la humanidad sea aniquilada por robots asesinos en 10 años*". La Razón.

LOS CIBERATAQUES DE RUSIA Y SU INFLUENCIA EN EL MARCO DEL CONFLICTO CONTRA UCRANIA EN EL AÑO 2022

Imagen: Representación ilustrativa de Ciber ataque Ruso.
Fuente: https://www.bbc.com/mundo/noticias-60850173

El presente trabajo de investigación, basado en el análisis de fuente abiertas, fue realizado como requerimiento académico en el marco del Curso de Capacitación y Perfeccionamiento para Jefes del año 2022. El mismo tiene por objetivo analizar y comprender la influencia que han tenido los ataques realizados dentro de lo que se considera el quinto dominio de la guerra, conocido como el ciber espacio, particularmente durante el inicio del conflicto armado iniciado entre Rusia y Ucrania.

INTRODUCCIÓN

El fenómeno de la globalización durante la década de los noventa y el surgimiento de internet como herramienta económica y social, han permitido que el intercambio de información y la velocidad de la misma, colaboraran en gran medida, a que la población estuviera más interconectada a nivel global y a un mayor desarrollo económico, cultural, social, político y militar. (Ibáñez, 2006)

La combinación de la rapidez, el libre acceso a la información y la dependencia permanente del acceso a internet de servicios esenciales, genera desde entonces nuevas amenazas a las infraestructuras críticas, desde el ciberespacio hacia sus expresiones físicas y tangibles, poniendo en riesgo a personas, organizaciones y países.

Es por ello, que se han tenido que reformular a nivel mundial, algunos conceptos de defensa y seguridad por parte de los estados (Ibáñez, 2006), considerando al ciberespacio como un nuevo dominio de la guerra para poder garantizar su soberanía respecto a las diferentes amenazas que pueden presentarse en este escenario, que desde el punto de vista del derecho internacional y las relaciones internacionales, surge la pregunta si, dentro de este nuevo espacio existe lugar para llevar a cabo un conflicto entre naciones.

Revista ECEME

MAYOR PABLO MARTÍNEZ

Oficial Jefe del Arma de Comunicaciones, actualmente Segundo Jefe del Bn. "Jura de la Constitución" de Com. Nº 2.

Es Diplomado en Estado Mayor y Licenciado en Ciencias Militares.

Prestó servicios en diferentes Unidades del Arma y en la Escuela Militar como Instructor y Jefe de Curso de Comunicaciones.

Participó de Misión Operativa de Paz como parte de los Contingentes en la República de Haití y República Democrática del Congo.

PALABRAS CLAVES

CIBERESPACIO
ESTRATÉGIA
DOCTRINA
CIBERATAQUE

DESARROLLO

Doctrina, estrategia y empleo militar de los ciber ataques rusos.

El 26 de febrero del año 2013, la figura del Jefe del Estado Mayor General de Rusia, el General Valery Gerasimov, llamó la atención al publicarse un artículo en la revista militar rusa Voyenno Promyshlennyy Kuryer (VPK), en donde expone su perspectiva del pasado reciente, presente y futuro esperado de la guerra. Allí se describe el marco para un nuevo concepto operativo durante los conflictos, donde se realizan y aplican medidas militares y no militares como ser, fuerzas especiales, fuerzas proxy, medios civiles y capacidades cibernéticas para poder influenciar, a favor o en contra, sobre quienes participan del conflicto, como también, interrumpir las comunicaciones o desestabilizar una determinada región. Este concepto operacional está compuesto por seis etapas (Imagen 1) y que se desarrollan a lo largo de todo el conflicto de acuerdo al siguiente orden: 1) Origen encubierto, 2) Escalada, 3) Actividades conflictivas, 4) Crisis, 5) Resolución y 6) Restablecimiento de la paz.

Existen diferentes medidas a aplicar durante todo el proceso, pero resulta importante resaltar que Gerasimov, considera que las conductas del conflicto de información, deben realizarse desde la primera etapa hasta la última, ubicándose en un gris entre medidas militares y no militares.

En este sentido, el ciberespacio, al ser un dominio transversal que interconecta y complementa otros ámbitos estratégicos, se ha convertido en un escenario clave para la ejecución de operaciones encubiertas y remotas (Bartles, 2016). Su naturaleza digital permite desarrollar acciones de conflicto de manera discreta y continua, difuminando la línea entre medidas militares y no militares, y redefiniendo así la forma en que se desarrollan los enfrentamientos en el siglo XXI.

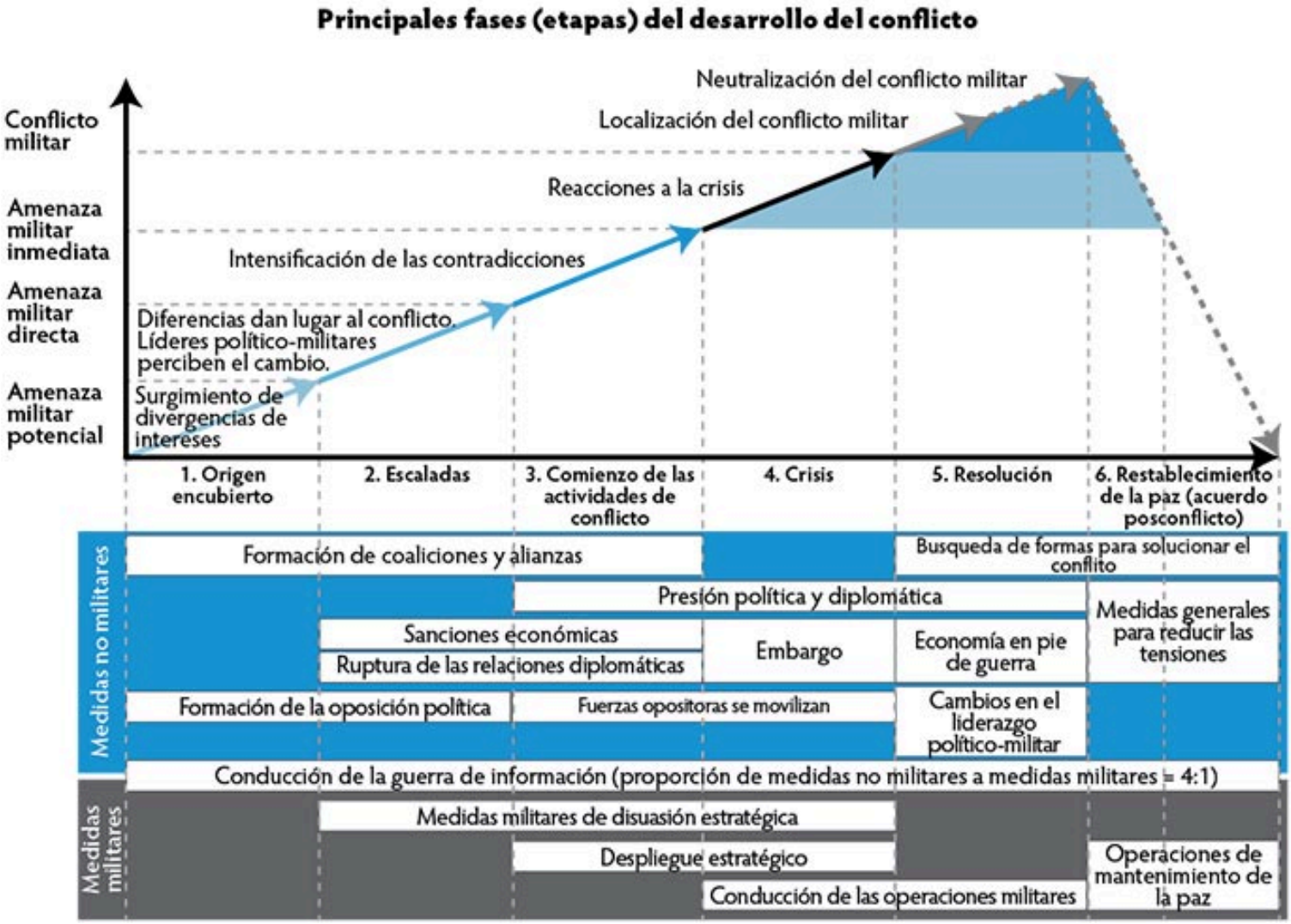

Imagen: Diseño Gráfico del nuevo concepto operativo.
Fuente: Charles K. Bartles, "Cómo comprender el artículo Gerasimov", Military Review, (2016)

Estrategia Militar Rusa

Una vez disuelta la Unión Soviética, Rusia ha tenido como prioridad dentro de su política exterior cercana, la protección y apoyo a las poblaciones rusas de otros ex estados soviéticos. (Zakem, 2022).

En este sentido, Rusia ha cambiado su visión respecto a los conflictos, considerando que las guerras ya no se declaran y el hecho que los elementos virtuales son tan importantes como los físicos, ha sido factor fundamental de su estrategia militar. (de Pedro, 2017). Es por ello, que algunos estrategas rusos han conceptualizado lo que se denomina guerra no lineal o guerra híbrida, como combinación de elementos virtuales y físicos. (de Pedro, 2017).

El profesor de Arte Operacional del Departamento de la Academia del Estado Mayor Ruso, Vasily Kopytko, identifica cinco períodos en la estrategia operacional rusa: primero de 1920 a 1940, con un empleo de las operaciones militares a gran escala y frontales; segundo hasta 1953, en donde los combates desarrollados en tierra eran apoyados por una potencia de fuego arrolladora, tercer periodo de 1954 a 1985, donde las armas nucleares tuvieron su protagonismo, el cuarto desde 1986 al año 2000, con el desarrollo de armas de alta precisión y largas distancias (misiles y artillería) y la quinta en donde actualmente se encuentra la estrategia rusa, dentro de dominios no tradicionales y con una combinación de medidas militares y no militares, conocida como guerra híbrida.

Se puede apreciar que la evolución de la estrategia militar rusa sugiere que el concepto tradicional de guerra ha quedado obsoleto frente a dinámicas de conflicto más fluidas y adaptativas. Más que una simple transformación tecnológica, se evidencia un cambio en la manera de concebir el poder y su proyección, donde la influencia estratégica se ejerce de manera difusa, sin necesidad de una confrontación directa. Esta lógica no solo redefine los umbrales de la agresión y la defensa, sino que también desafía las estructuras de seguridad internacional, obligando a otros actores a repensar sus propios enfoques frente a amenazas que no siempre son visibles ni inmediatas.

División Cibernética Rusa

Respecto al origen de los protagonistas que llevan adelante las operaciones cibernéticas rusas, Dmitry Rogozin, quien se desempeñó desde el año 2011, como encargado de los proyectos de investigación avanzada en materia de defensa, menciona a las ciber tropas públicamente por primera vez en el año 2012. Sin embargo, en el año 2000 cuando se adoptó la primera doctrina de seguridad de la información, la misma ya destacaba la necesidad de proteger y resguardar a la población rusa de la información externa perjudicial, sin hacer referencia explícita a las acciones ofensivas en este nuevo dominio. Por otra parte, Nativ Yakov, quien cumplió funciones como Jefe del Servicio de Inteligencia Israelí, manifestaba que en todos los Ejércitos serios las ciber tropas están presentes, las cuales desarrollan tareas propagandísticas y operacionales, definiéndolas como actividades que tienen por finalidad distraer a los adversarios, haciéndoles caer en errores a través de campañas de desinformación. Rusia no ha sido la excepción, de hecho en el año 2013, el ministro de defensa ruso Sergei Shoigu, anunció una gran cacería de programadores debido al enorme volumen de software que el Ejército necesitaría desarrollar en los próximos cinco años. (Popsulin, 2013).

En el año 2014, el ministerio de defensa crearía Cyber Command, como una nueva rama de las fuerzas armadas para contrarrestar las amenazas virtuales, aunque esta unidad no sería reconocida por Rusia hasta el año 2017. En el mes de enero de ese mismo año, el estudio analítico Zecurion Analytics, expresó que Rusia se encuentra dentro de los cinco primeros países en número y financiación de ciber tropas. Las mismas se estiman en 1.000 militares y con un presupuesto anual de U$S 300 millones. Respecto a su estrategia, inicialmente los primeros ataques cibernéticos eran llevados a cabo por agentes privados con el apoyo de Rusia. Hoy día existe una planificación y coordinación, para que el ciber espacio este gestionado en forma más eficaz por instituciones como el FSB (Servicio Federal de Seguridad) y el propio Ministerio de Defensa. Sin embargo, muchas de las actividades cibernéticas terminan siendo realizadas por grupos de hackers, como Fancy Bear o Cozy Bear entre otros, con una previa coordinación del FSB y el Ministerio

de Defensa. La GRU (Dirección Principal de Inteligencia), tiene por finalidad dirigir la contra información y las operaciones sicológicas, aunque su mayor fortaleza está en la combinación de las operaciones cibernéticas, electrónicas y sicológicas. Con respecto a otras divisiones cibernéticas del estado ruso, la GRU tiene una perspectiva estratégica a largo plazo, realizando acciones para socavar y degradar a sus oponentes, pero particularmente, mantener una influencia favorable dentro del ciber espacio.

Si bien estas unidades vienen realizando operaciones cibernéticas desde la primera invasión rusa en el año 2014, dificulta saber en qué momento cambiaron su estrategia de espionaje a largo plazo para apoyar la preparación de la actual invasión.

Los ciber ataques Rusos, antecedentes y actuales.

Si bien los dominios terrestre, aéreo o marítimo, pueden resultar ser los más visibles y tangibles durante un conflicto, como ser el bombardeo a ciudades o tropas y vehículos avanzando por territorio invadido, la dimensión ciber espacial es la que menos trascendencia puede llegar a tener considerándolo desde una mirada propagandística o noticiosa.

Por lo que amerita recontar los múltiples ataques cibernéticos que ha recibido Ucrania desde mucho antes del actual conflicto, si se quiere como una antesala de lo que sucedería el pasado 24 de febrero del presente año.

Como antecedentes y siendo consecuente con los acontecimientos políticos desde el año 2013, se describirán las siguientes acciones realizadas por el componente cibernético ruso:

Año 2013: Operación Armagedón; tenía como objetivo los sistemas de información, tanto de instituciones privadas como gubernamentales de Ucrania. (Gonzalo, 2022).

Año 2014: Snake o la Serpiente Griega Ouroboros; la compañía británica de defensa y seguridad BAE Systems, informó que docenas de redes informáticas del gobierno ucraniano habían sido objeto de ciber ataques. (Gonzalo, 2022).

Desde 2014 a 2016: Fancy Bear y los obuses D-30 Howitzer Fancy Bear o APT28, es un grupo de hackers que desde el año 2014 al 2016, utilizó un malware en una app de Android, que le permitió atacar a las fuerzas de cohetes y artillería del Ejército ucraniano, controlando particularmente, la información de puntería del obús D-30 Howitzer y afectando a más del 80% de este armamento. (Gonzalo, 2022).

Año 2017: NotPetya, el más destructivo; este ataque cibernético es considerado el más destructivo y costoso de la historia. Si bien fue dirigido por Rusia hacia Ucrania, el mismo se extendió hacia otros países ocasionando pérdidas de 10.000 millones de dólares a empresas multinacionales como la naviera Maersk, FedEx y la farmacéutica Merck, entre otras. (Gonzalo, 2022).

Año 2021: Covid-19 como cebo; en abril de 2021 organizaciones relacionadas con la seguridad de Ucrania, sufrieron un ataque de phishing, en donde se utilizaban cebos de ingeniería social en los asuntos de los correos electrónicos (Gonzalo, 2022).

Año 2022: el 14 de enero, dos días después de que Rusia rompiera relaciones diplomáticas con occidente, visualizando una posible invasión a Ucrania, 70 sitios web gubernamentales ucranianos entre los cuales se encontraban el gabinete de ministros, ministerios de educación, energía, agricultura, ecología y asuntos exteriores, se vieron afectados por ciber ataques del tipo de denegación de servicios. (Gonzalo, 2022).

14-15 de febrero de 2022; similar al ciber ataque de un mes atrás, los sitios web estatales de las fuerzas armadas fueron atacados por ciber ataques, Ministerio de Defensa y del sector financiero como Oschadbank y Privatbank, considerados las principales entidades bancarias del país. (Gonzalo, 2022).

24 de febrero de 2022; coincidiendo con el anuncio del Presidente de la Federación de Rusia de una "operación militar especial" en Ucrania, un ciber ataque masivo sobre infraestructuras digitales de Ucrania, provocó que varios páginas webs de importancia para del gobierno, como el gabinete de ministros, ministerio de asuntos exteriores y de educación, quedaran inoperativos. (Gonzalo, 2022).

CONCLUSIONES

De acuerdo a los conceptos, antecedentes y hechos presentados durante el desarrollo, puede quedar la

percepción que Rusia se encuentra ganando la guerra en este dominio. Sin embargo, sus ataques han sido demasiado específicos y de una complejidad técnica no muy sofisticada, ya que considerando el tiempo de preparación, los recursos económicos, materiales y humanos, junto a la doctrina de la guerra de la información planteada por el General Gerasimov, se esperaría que Rusia ejecutara operaciones para realizar prácticamente un apagón informático con consecuencias devastadoras ante una debilitada Ucrania, pero a pesar de ello no ha resultado de esa manera. Naturalmente surge la pregunta, respecto al hecho que Rusia aun no haya desplegado su potencial para realizar operaciones cibernéticas de mayor escala. En este sentido, ¿será que no es su voluntad por el momento o quizás no tenga la capacidad?

Es verdad que el empleo del ciber espacio por parte de Rusia en algunas campañas de sabotaje, espionaje o denegación de servicios, han resultado en forma exitosa (Gonzalo, 2022), pero quizás esos hechos nos han llevado a sobrevalorar ampliamente sus capacidades, porque de tener esa posibilidad, puede resultar extraño que Rusia no despliegue todo su potencial para evitar que el conflicto se prolongue aún más en el tiempo, ante los ojos de la comunidad internacional (incluido parte del pueblo ruso), que cuestionan la invasión.

Quizás el hecho de que los ataques sean de baja complejidad técnica y sus efectos sean de corto plazo, puede estar contribuyendo a que estén perdiendo efectividad, tomando en cuenta que sus técnicas ya son demasiado conocidas. De igual manera, sucede con las campañas de desinformación, en donde diferentes medios de comunicación y redes sociales en el mundo, han restringido la difusión de los canales de información rusos, como RT o Sputnik, mermando significativamente la capacidad de influir sobre la opinión pública internacional. (Taube, 2022).

Por su parte y ante la ofensiva rusa, Ucrania ha sido respaldada y apoyada por estados, organizaciones y compañías, principalmente Microsoft y Space X, (Endicott, 2022), lo que le permitió mejorar su mando de ciber defensa de forma cuantitativa y cualitativa, (Endicott, 2022). como así también, reducir las vulnerabilidades de sus servicios esenciales e infraestructuras críticas. De esta manera, ha logrado mantener la operatividad y conectividad a nivel gubernamental, social, económico y militar en lo que va del conflicto.

Quizás la visión estratégica de Rusia de evitar efectos colaterales impredecibles a terceros países, como ocurrió con NotPetya en el año 2017, podría ser otro de los argumentos que la han llevado a no emplear al máximo sus ciber capacidades ofensivas. De esta manera, es probable que el Moscú no quiera extender el conflicto a otros estados, particularmente de la OTAN y haya desistido por el momento, de emplear sus capacidades cibernéticas en forma amplia y sin escrúpulos, considerando también que tiene la situación razonablemente controlada.

La incidencia de los ciber ataques rusos fueron importantes al inicio de la invasión, particularmente al momento de combinarlos con acciones militares sobre objetivos estratégicos, sin embargo, están siendo menos determinantes en este momento del conflicto, ya que están jugando un papel mucho menos relevante y decisivo, de acuerdo a su tiempo de preparación, la inversión en recursos humanos y materiales realizada, considerando también, que los efectos de sus ataques y su sorpresa se diluyen conforme pasa el tiempo.

A pesar de ello, la importancia de las actividades realizadas en el ciber espacio durante el presente conflicto y en los que se avecinarán en el futuro, será cada vez mayor y quien tenga superioridad en este dominio, dada su transversalidad, podrá afectar y dominar el resto de los espacios físicos de forma eficaz para poder obtener la ventaja estratégica.

Referencias Bibliográficas

De Vergara, Evaristo y Trama, Gustavo Adolfo. (2017) Operaciones Militares Cibernéticas.
Bartles, Charles (2016). "Cómo comprender el artículo de Gerasimov". Military Review.
Colom Piella, Guillem (2018). "La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo".
Ibáñez, Josep (2006). "Globalización e Internet: poder y gobernanza en la sociedad de la información".
Selhorst, Tony, Lt. Col. (2016) "Russia´s Perception Warfare. The development of Gerasimov's doctrine in Estonia and Georgia and it's application in Ukraine".
de Pedro, Nicolás. (2017) "Rusia se apunta a la guerra híbrida".
Endicott, Sean. (s.f.). "Microsoft ha comprometido más de $ 35 millones para ayudar a Ucrania".
Frisby, Josué. (2020). "Índice de exposición a la Ciberseguridad (CEI) 2020"
Gonzalo, Marilín. (2022). *"Rusia –Ucrania: Cronología de una ciberguerra"*.
Interfax. (s.f.) *"El Ministerio de Defensa de la Federación Rusa creó las tropas de operaciones de información"*.
Kommepcahtb. (s.f.) *"Tropas de operaciones de información creadas en Rusia"*.
Microsoft. (s.f.) *"Special Report: Ukraine. An overview of Russia´s cyberattack activity in Ukraine"*.
Sukhankin, Serguéi. (s.f.) *"Ciber tropas rusas: un arma de agresión"*.
Sukhankin, Serguéi. (s.f.) *"Rusia refuerza sus capacidades cibernéticas ofensivas"*.
Taube, Friedle. (s.f.) *"Guerra en Ucrania: ¿qué papel juegan los ciberataques?"*.
Turovski, Daniil. (2016). *"Fuerzas cibernéticas armadas rusas. Como el estado crea destacamentos de piratas informáticos"*.

Integración e Interacción multiagencial en la Ciberseguridad y Ciberdefensa a nivel Nacional e Internacional.

IMAGEN: Unidad de Ciberdefensa del Ejército .
FUENTE: https://www.ejercito.mil.uy/index.php/tag/ciberseguridad/

El presente artículo se enmarca en el trabajo de investigación del año 2022, llevado a cabo en la E.C.E.M.E. El mismo tiene por objetivo analizar la integración e interacción de diferentes agentes nacionales e internacionales en materia de ciberseguridad y ciberdefensa, en el contexto del conflicto entre Rusia y Ucrania, donde el ciberespacio aumenta protagonismo como dominio estratégico de confrontación.

INTRODUCCIÓN:

La evolución en las tecnologías de la información ha llevado a que en los conflictos bélicos se hable de la existencia de un nuevo dominio denominado Ciberespacio, el cual está conformado por todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. (Richard A. Clarke, 2011)

No se trata solo de internet -es importante dejar en claro la diferencia- Internet es una red de redes abierta, en la que cualquier ordenador conectado puede comunicarse con otro, siempre que no existan restricciones de seguridad, permisos o configuraciones específicas que lo impidan. (Richard A. Clarke, 2011)

Internet es una vasta red de redes interconectadas que permite la comunicación global entre dispositivos, sin importar su ubicación. Cada ordenador conectado a esta infraestructura forma parte de un entramado digital que posibilita el intercambio de información con otros equipos, siempre que no existan restricciones de seguridad o configuraciones que lo impidan.

Más allá de esta red global, se encuentra el ciberespacio, un dominio que comprende no solo Internet, sino también otras redes privadas que, en teoría, no son accesibles desde ella. Algunas de estas redes cerradas reproducen el funcionamiento de Internet, pero permanecen separadas de esta, configurando un ecosistema digital en el que la información circula con distintos niveles de acceso, seguridad y confidencialidad.

En conjunto, estas dimensiones conforman el escenario en el que se

Revista ECEME

MAYOR FABIAN GORDIOLA

Oficial Jefe del Arma de Comunicaciones, actualmente Segundo Jefe del Bn. "Libertad o Muerte" de Com. N°1.

Es diplomado en Estado Mayor y Licenciado en Ciencias Militares.

Prestó servicio en diferentes Unidades del Arma, en el Liceo Militar "General Artigas" y en la Escuela de Capacitación y Perfeccionamiento de Personal Superior de las Armas del Ejército como Instructor.

Participó en Misión Operativa de Paz como parte del Contingente en la República Democrática del Congo y como Ayudante del Jefe de Misión en India y Pakistán

PALABRAS CLAVES

CIBERESPACIO
ESTRATÉGIA
CIBERSEGURIDAD
CIBERDEFENSA

desarrollan el conocimiento, la colaboración y la innovación en la era digital.

En este tejido, el ciberespacio no solo es un entorno de intercambio de información y desarrollo tecnológico, sino también un nuevo escenario estratégico en el que se configuran dinámicas de poder y conflicto. Aparte del plano terrestre, marítimo, aéreo y espacial, la guerra ha entrado en el quinto dominio: el ciberespacio. Es donde el hombre alcanza a través de impulsos electromagnéticos mediante el uso de elementos informáticos.

Por ejemplo, cuando se habla de ciberataques, se debe pensar no solo en un simple virus que pueda dañar alguna información de carácter digital, los que mediante el uso de medidas de ciberseguridad se pueden resolver, sino que potencialmente implica la paralización del sistema económico de un país o la afectación de todo un equipamiento u organización, por su grado de complejidad y afectación a nivel estratégico, queda en el marco de la Defensa Nacional.

La interconectividad que existe hoy en el mundo, donde la información viaja de un extremo a otro a velocidad imperceptible para el hombre por lo que su dominio es casi o totalmente imposible. Solo pensar en la posibilidad que existe de poder estar conectados en tiempo real a pesar de la distancia geográfica, nos puede dar una idea de la significancia que tiene hoy el internet y su conexión a través de ella. Esas facilidades son las que nos han hechos vulnerables ante la exposición que tenemos en el internet, canal conductor del ciberespacio.

IMAGEN: Articulo de diario sobre el conflicto en el ciberespacio.
FUENTE: https://es.andersen.com/es/publicaciones-y-noticias/el-conflicto-belico-de-ucrania-generado-por-la-invasion-rusa-vive-un-conflicto-paralelo-en-el-ciberespacio.html

DESARROLLO

La ciberdefensa al pasar de los años se ha ido incorporado de forma vertiginosa a nivel mundial (Silvina Conaglia, 2017), de manera tal que los ataques cibernéticos son moneda corriente no solo contra las infraestructuras criticas, sino que trasciende a la población en general, más específicamente al usuario común.

Diversos casos de gran impacto han servido como detonantes para la adopción de medidas que trascienden el ámbito de la ciberseguridad, convirtiéndose en estrategias de defensa nacional. Estos incidentes han afectado múltiples sectores, incluyendo la prensa, el sistema financiero, entidades gubernamentales, plantas nucleares y la filtración de información clasificada, evidenciando la vulnerabilidad de infraestructuras críticas ante amenazas digitales.

Paralelamente, el lenguaje ha evolucionado para reflejar la creciente convergencia entre la cibernética y las actividades ilícitas, dando lugar a términos como cibercrimen, ciberterrorismo y ciber-espionaje, mientras que, en contraposición a la ciberdefensa y emergió la ciberguerra. Sin embargo, la complejidad de estas amenazas va más allá de una simple redefinición teórica; sus consecuencias pueden ser impredecibles en alcance e impacto, con perpetradores que a menudo resultan irrastreables e indetectables. Esta realidad se ve favorecida, en parte, por la falta de un marco legal unificado para regular el ciberespacio, lo que ha impulsado a organizaciones supranacionales, estados y entidades no gubernamentales a abordar el problema no solo de manera individual, sino también a través de mecanismos de cooperación, como tratados y acuerdos internacionales.

El ciberespacio como nuevo dominio de conflicto

El ciberespacio se ha consolidado como el quinto dominio de la guerra (Richard A. Clarke, 2011), junto con los ámbitos terrestre, marítimo, aéreo y espacial. En este entorno, los ataques informáticos no solo buscan comprometer la seguridad de los datos, sino también

generar caos económico, alterar infraestructuras esenciales y erosionar la confianza en las instituciones gubernamentales.

Los ataques cibernéticos afectan a la defensa militar cuando son orientados exclusivamente con el propósito de limitar o neutralizar las capacidades militares dentro de un escenario bélico, en sentido se puede decir que apunta hacia sus sistemas de información y comunicaciones militar. En otros puntos de vista refieren a aquellos ataques cuyo objetivo son afectar la infraestructura militar y naval del enemigo, la logística y sus cadenas de suministros, distraer, confundir e inhabilitar el sistema C4IVR (Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento), desigualar las capacidades del enemigo y crear la oportunidad para acciones de ataques sobre objetivos estratégicos en sus infraestructuras críticas.

La guerra cibernética presenta desafíos únicos, ya que permite a los agresores atacar sin revelar su identidad, empleando tácticas de desinformación, sabotaje digital y manipulación de la percepción pública. Además, los efectos de un ciberataque pueden propagarse rápidamente a nivel global, afectando no solo a los países involucrados en el conflicto, sino también a entidades privadas y sectores económicos enteros.

El caso del conflicto Rusia-Ucrania ha puesto en evidencia cómo los ataques informáticos pueden debilitar la capacidad operativa de un país, interrumpiendo servicios esenciales como la energía, el transporte y las telecomunicaciones. Esta guerra ha demostrado que la ciberdefensa debe ser una prioridad estratégica para cualquier nación que busque mantener su soberanía digital y garantizar la estabilidad de sus infraestructuras críticas.

Estrategias de ciberdefensa de Ucrania

Frente a al contaste ataque cibernético recibido por Ucrania a lo largo de los años y la intensificación durante el avance del conflicto, Ucrania ha adoptado diferentes medidas las cuales hemos ido desarrollando en nuestro trabajo de investigación y explicaremos algunos en el presente artículo:

1. Cooperación con aliados internacionales: La colaboración con la OTAN, Estados Unidos y la Unión Europea ha permitido fortalecer la seguridad digital de Ucrania mediante la transferencia de tecnología, inteligencia y capacitación especializada. (Departamento de Seguridad Nacional, 2022)
2. Fortalecimiento de la infraestructura digital: Se han implementado sistemas de detección temprana de amenazas y mecanismos de recuperación ante incidentes, reduciendo el impacto de futuros ciberataques. (D. Iriarte, 2022)
3. Colaboración con el sector privado: Empresas como Microsoft, Google y Cisco han desempeñado un papel clave en la protección de los sistemas informáticos ucranianos, bloqueando intentos de intrusión y facilitando la identificación de nuevas tácticas de ataque. (IT Master Mag, 2022)
4. Creación del IT Army of Ukraine: Un esfuerzo sin precedentes en el que voluntarios internacionales se unieron para lanzar contraataques digitales contra objetivos estratégicos rusos. (S. Soezanto, 2022)
5. Seguridad digital: Implementación de servidores en el extranjero para la protección de datos gubernamentales y adopción de tecnologías en la nube para garantizar la continuidad operativa en caso de ataques masivos. (B.Smith, 2022)

Impacto global de la guerra cibernética

El conflicto entre Rusia y Ucrania ha demostrado que la guerra cibernética no se limita a los países directamente involucrados, sino que tiene implicaciones globales (B. Smith, 2022). Algunos de los efectos más relevantes incluyen:

- Incremento de los presupuestos en ciberseguridad: Gobiernos de todo el mundo han reforzado sus inversiones en la protección de infraestructuras

digitales ante la creciente amenaza de ataques cibernéticos. (B. Valeriano y E. Lonergan, 2022)

- Cooperación internacional en ciberdefensa: Se han establecido acuerdos multilaterales para compartir información sobre amenazas cibernéticas y desarrollar respuestas conjuntas ante ataques de gran escala. (B. Smith, 2022)
- Evolución de la guerra híbrida: El caso ucraniano ha evidenciado que los conflictos modernos requieren una combinación de estrategias militares y cibernéticas para ser efectivos. (B. Smith, 2022)

Lecciones aprendidas y desafíos futuros

El conflicto Rusia-Ucrania ha dejado múltiples enseñanzas en el ámbito de la ciberdefensa, entre ellas:

- La ciberseguridad debe ser una prioridad nacional: Las infraestructuras críticas de cualquier país pueden convertirse en objetivos de ataques cibernéticos, por lo que su protección es fundamental. (S. Cornaglia y A. Vercelli, 2017)
- La cooperación internacional es clave: La resiliencia digital no puede lograrse de manera aislada; requiere el trabajo conjunto de gobiernos, organizaciones y empresas tecnológicas. (M.Pessino, 2017)
- El ciberespacio seguirá siendo un campo de batalla en el futuro: A medida que la tecnología avance, es probable que los ciberataques se vuelvan más sofisticados y difíciles de rastrear. (S. Cornaglia y A. Vercelli, 2017)

El conflicto actual ha sentado un precedente en la forma en que se desarrolla la ciberguerra, estableciendo un modelo de referencia para futuras confrontaciones en el ámbito digital. La capacidad de anticiparse a las amenazas y la colaboración entre actores clave serán esenciales para mitigar los riesgos asociados a la guerra cibernética en los próximos años.

CONCLUSIONES

La evolución de las tecnologías de la información y sus componentes de manejo van creciendo de forma acelerada, es por ello que los estados deberán acompañar este avance de manera de estar a la vanguardia de los medios y métodos que atienden a la Ciberseguridad y la Ciberdefensa, no solo con el fin de proteger la información sensible de los habitantes, de un estado o una nación del ataque a sitios web del gobierno, sino que también deben poseer e implementar sistemas de defensa para la protección de infraestructuras críticas, objetivos claves en un conflicto bélico, las cuales se han convertido en dependientes de la internet y por consiguiente participes activos del ciberespacio, resultando un mayor impacto ante eventuales ataques.

La vulnerabilidad que se encuentra en el ciberespacio a través de ciberataques, demuestra que se hace imperioso una mayor integración de los agentes internacionales así como también su cooperación en materia de ciberseguridad y ciberdefensa. En esta ocasión quedó demostrado como Ucrania tras varios años bajo ataques cibernéticos ha logrado estar a la vanguardia de modo tal que los efectos o daños que pudiera sufrir son disminuidos en su afectación mediante la implementación de diferentes acciones.

Si bien las grandes potencias tienen un gran poderío de armamento bélico, no son ajenos a este nuevo dominio que se utiliza en los conflictos modernos, más aún cuando la interconexión a través del internet hace que por efecto rebote el alcance de un ataque sea a nivel internacional en mayor o menor medida e impredecible, por lo que son igual de vulnerables. Las medidas que se toman para el dominio de seguridad de las redes a nivel regional e internacional deben ser actualizadas constantemente para mitigar al máximo un ciberataque y es por ello que la integración de la agencias de ciberdefensa internacional es fundamental para que la evolución sea de forma integrada.

Generalmente en un conflicto bélico de carácter convencional se intenta excluir al componente civil, pero dentro de un ciberataque, este es el objetivo inicial, por lo que la concientización de las personas es fundamental para la seguridad a nivel nacional como internacional, porque como en el conflicto aún latente de Rusia-Ucrania, los objetivos principales fueron instituciones de gobierno, empresas internacionales, personas y además componentes militares.

Referencias Bibliográficas

Pessino, Mauro. (2017) *"Las Políticas en ciberseguridad de la Organización del Tratado (OTAN). Período 2008 - 2013"*.

Alonso, Rodrigo. (2022). *https://www.elcorreo.com/internacional/europa/army-anonymous-brigadas20220314065851-*.

Anaya, Fernando. (2022). *https://globbsecurity.com/cumbre-de-la-otan-estas-son-las-claves-en-ciberseguridad48502*.

Burt, Tom. (2022). *https://news.microsoft.com/es-xl/laguerra-hibrida-en-ucrania/*.

Camps, Pablo. (2019) *"Ciberdefensa y ciberseguridad: nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias de este ámbito"*.

Colom Piella, Guillem. (2018). *"La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo"*.

Sergio g. Eissa, Sol Gastaldi, Iván Poczynok, Elina Zacarías Di Tujillo. (2014) *"El ciberespacio y sus implicancias para la defensa nacional"*.

PROSPECTIVA ESTRATÉGICA: FORTALECIMIENTO DE LA CIBERDEFENSA Y LA SEGURIDAD NACIONAL DEL URUGUAY

Imagen: Unidad de Ciberdefensa del Ejército Nacional
Fuente: Dpto. Comunicación Institucional del Ejército Nacional

En el marco del Curso de Estado Mayor del Instituto Militar de Estudios Superiores (IMES) y bajo la supervisión del Centro de Estudios Jurídicos y Estratégicos (CEJE), se desarrolló en el 2021 el proyecto de prospectiva "Aldebarán".

Este artículo presenta un análisis del proyecto "Aldebarán", un innovador trabajo de prospectiva estratégica llevado a cabo en el año 2022, y su relación con los hallazgos de la investigación titulada "Ciberdefensa: su relación con las infraestructuras críticas y el problema de la seguridad nacional".

Cada alumno participante del curso recibió un tema relevante asignado por el IMES. En el caso de esta investigación, el tema fue la ciberdefensa y su impacto en las infraestructuras críticas del país. Guiados por tutores expertos, los oficiales desarrollaron una base teórica conceptual que sirvió como sustento para el análisis prospectivo.

La ciberdefensa y la protección de las infraestructuras críticas se han convertido en pilares fundamentales de la seguridad nacional en el siglo XXI (Consejo Argentino para las Relaciones Internacionales, 2022). Conscientes de este desafío, el Ejército Nacional de Uruguay ha emprendido importantes iniciativas orientadas al desarrollo de capacidades prospectivas y tecnológicas (Poder Ejecutivo, 2020).

Durante el proceso, se identificaron dos Tendencias Estratégicas Posibles (TEPos) y, tras aplicar los métodos "Acuña-Konow" y "Delpho", se determinó una Tendencia Estratégica Probable (TEPro) que se evaluó utilizando la Matriz de Impactos Estratégicos (MIE).

La investigación desarrollada en el marco del proyecto "Aldebarán" aborda la

Revista ECEME

MAYOR RÚBEN CASTALDI

Oficial Jefe del Arma de Artillería, actualmente se desempeña como Jefe de Curso de Artillería en la Escuela de Capacitación y Perfeccionamiento del Personal Superior de las Armas de Ejército.

Es diplomado en Estado Mayor y Licenciado en Ciencias Militares.

Prestó servicio en diferentes unidades del Arma de Artillería.

Participó de Misión Operativa de Paz como parte de los Contingentes en la República de Haití y República Democrática del Congo

PALABRAS CLAVES

PROSPECTIVA
ESTRATÉGIA
CIBERESPACIO
CIBERDEFENSA

ciberdefensa como un elemento esencial para la protección de las infraestructuras críticas del país.

Estas infraestructuras, que incluyen sectores como energía, telecomunicaciones y finanzas, son cada vez más vulnerables a los ciberataques (Rico, 2021), debido a su creciente dependencia de sistemas digitales.

La investigación identificó que, si bien Uruguay ha avanzado en la creación de marcos normativos y unidades especializadas como el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) y la Unidad de Ciberdefensa del Ejército (U.CIBER.E.), aún existen desafíos importantes en términos de coordinación interinstitucional y desarrollo de capacidades tecnológicas (Castaldi, 2022).

El análisis prospectivo permitió determinar que, en el corto y mediano plazo, la implementación de estrategias de ciberdefensa integradas será clave para garantizar la soberanía digital del país. Además, se concluyó que el fortalecimiento de la colaboración entre el sector público y privado es fundamental para mitigar los riesgos asociados a los ciberataques.

> ***Uruguay avanza en la protección del ciberespacio mediante estrategias nacionales de ciberdefensa e innovación tecnológica.***

El proyecto "Aldebarán" y su aplicación a la ciberdefensa demostró el potencial de esta metodología para analizar situaciones relevantes y anticipar escenarios.

El proyecto "Aldebarán" contribuyó al fortalecimiento de la capacidad prospectiva del Ejército Nacional, y también mediante un ejercicio académico validó las bases para el desarrollo de una estrategia de ciberdefensa integral que garantice la seguridad y soberanía del país en el entorno digital, visualizado como más complejo riesgoso y sustancial.

Imagen: Unidad de Ciberdefensa del Ejército Nacional
Fuente: Dpto. Comunicación Institucional del Ejército Nacional

Referencias Bibliográficas

Castaldi, R. (2022). *"Ciberdefensa: su relación con las infraestructuras críticas y el problema de la seguridad nacional"*.
Consejo Argentino para las Relaciones Internacionales. (2022). "Ciberseguridad y Ciberdefensa en América Latina".
Poder Ejecutivo. (2020). *Política de Defensa Nacional 2020-2025*.
Rico, J. (2021). *Marco normativo para la protección de infraestructuras críticas*.

EMPLEO DE LA INTELIGENCIA POR PARTE DEL EJÉRCITO EN LAS ACTIVIDADES DE PATRULLAJE FRONTERIZO.

Situación de los Ejércitos de Argentina y Brasil.

Imagen: Estado Mayor de la Defensa
Fuente: Ministerio de Defensa Nacional - Estado Mayor de la Defensa. https://www.gub.uy/ministerio-defensa-nacional/esmade

Revista ECEME

TENIENTE CORONEL MARTÍN LOPEZ

Oficial Jefe del Arma de Infantería, actualmente Jefe del Cuartel Gral. de la Brigada "Gral. José de San Martín" de Infantería Nro 2.

Prestó servicio en diferentes unidades del Arma de Infantería.

Diplomado en Estado Mayor y Licenciado en Ciencias Militares

Participó de Misión Operativa de Paz como parte de los Contingentes en la República de Haití y República Democrática del Congo

PALABRAS CLAVES

PROSPECTIVA
OPERACIONAL
INTELIGENCIA MILITAR

INTRODUCCIÓN

Desde el año 2020, en nuestro país se estableció la participación de las Fuerzas Armadas en tareas de vigilancia y apoyo a diversas instituciones dentro de una franja fronteriza de 20 km. para garantizar un empleo eficiente de los recursos humanos y materiales, considerando muy importante el intercambio de información con los países limítrofes. (Ley 19.677, 2018)

En este artículo se presenta un análisis del Proyecto "Aldebarán", el cual, mediante el uso de un software especializado y un estudio prospectivo estratégico, permite crear tendencias estratégicas, las cuales son evaluadas y analizadas y posteriormente arrojan conclusiones al respecto.

Metodología Prospectiva "Proyecto Aldebarán"

El Centro de Estudios Jurídicos y Estratégicos desarrolló un software para identificar y analizar tendencias estratégicas en distintos factores del poder nacional. Como alumno externo y Oficial de Operaciones de la Brigada "Gral. José de San Martín" de Infantería N.° 2, recibí el tema sobre: El empleo de la inteligencia en el patrullaje fronterizo,en la situación de los Ejércitos de Argentina y Brasil.

Guiados por tutores expertos, se estableció una base teórica conceptual para realizar un estudio prospectivo. Se identificaron dos Tendencias Estratégicas Posibles (TEPos) y, mediante la aplicación de los métodos "Acuña-Konow" y "Delpho", se definió una Tendencia Estratégica Probable (TEPro), la cual fue evaluada a través de la Matriz de Impactos Estratégicos (MIE) y se la cruzó con 6 indicadores estratégicos del Factor Militar y su grado de afectación.

BASE TEÓRICO CONCEPTUAL

Marco Legal

Se destacan los acuerdos con Argentina, enfocados en la delimitación de los ríos de la Plata y Uruguay, la cooperación y el desarrollo de zonas fronterizas, además de

la vigilancia aérea conjunta. (TRATADO DE LIMITES DEL RIO DE LA PLATA Y SU FRENTE MARÍTIMO, 1974) (C.A.R.U., 2019)

Con Brasil, sobresalen convenios para la reducción del tráfico de estupefacientes y la cooperación transfronteriza. (Ley 16.424, 1993) (Ley 17.095, 1999)

A nivel nacional, la Ley Marco de Defensa Nacional y los Decretos N.º 129/196 y 371/020 promueven el intercambio de información y la realización de acciones y ejercicios combinados para fortalecer la seguridad y la defensa. (Ley 18.650, 2010)

Antecedentes

Las Fuerzas Armadas han participado en varios ejercicios conjuntos con países de la región, destacando la Operación Ceibo con el Ejército Argentino y maniobras de misiones de paz con el Ejército Brasilero. Asimismo, se han reforzado las fronteras en eventos internacionales como el G20 en Argentina y el Mundial de Fútbol y Olimpiadas en Brasil.

Hechos relevantes

Desde el inicio de las Operaciones de Frontera Segura, el Ministro de Defensa Nacional se ha reunido con sus homónimos de Argentina y Brasil para reforzar la vigilancia fronteriza e incrementar el intercambio de información y experiencias.

Imagen: Puesto de Control de Ruta en Op. Frontera Segura.
Fuente: Dpto. Comunicación Institucional del Ejército.

Tendencias Estratégicas Posibles

Las Tendencias Estratégicas Posibles formuladas fueron las siguientes:

1. TEPos Nro. 1: Fortalecimiento y consolidación del intercambio de información entre los distintos Ejércitos
2. TEPos Nro. 2: Regulación del marco legal para el intercambio de información, entre los Ejércitos.

Cada una de estas Tendencias fue identificada y delimitada, se analizaron los efectos inmediatos, deseados y ulteriores.

Posteriormente el autor define los Elementos de la Fórmula "Acuña y Konow" (Tendencia Histórica, Eventos en curso y Hechos Portadores de futuro) y genera conclusiones parciales para cada uno de ellos y un coeficiente que sumados los tres debe dar igual a 1, seguidamente la totalidad de los participantes evalúa el resultado presentado a través del software y se genera un promedio final para ambas TEPos.

Seguidamente se somete la TEPos al Método Delpho en donde nuevamente la totalidad de los participantes del proyecto evalúa el resultado obtenido en las etapas anteriores, de los promedios de sus estimaciones, se consideran aspectos como el porcentaje de la probabilidad de ocurrencia, la pertinencia de la misma para la Institución, y el promedio de las autoevaluaciones de los participantes. Este consenso, le da estabilidad a las TEPos. y a partir de ahora se pueden considerar Tendencias Estratégicas Probables (TEPros) permitiendo obtener una previsión de futuro cuantificada, con el fin de servir de apoyo para la toma de decisiones.

Tendencia Estratégica Probable

La transformación de la TEPos. en TEPros. hace que se la pueda someter al análisis de la Matriz de Impactos Cruzados donde se expone la misma a los elementos seleccionados del Factor Militar para determinar cómo los efectos inmediatos, deseados y ulteriores interactúan.

La TEPos Nro. 1: "Fortalecimiento y consolidación del intercambio de información entre los distintos Ejércitos", fue la seleccionada, la cual se convierte en Tendencia Estratégica Probable Nro. 1.

Matriz de Impactos Estratégicos

Una vez identificada la TEPro, posteriormente se la analiza mediante la Matriz de Impactos Estratégicos, en la cual se la cruza con 6 indicadores estratégicos del Factor Militar y su grado de afectación, a continuación, se expresarán los resultados de mencionado análisis:

- Para el Indicador Estratégico Nro. 1: "Capacidad operacional para la misión fundamental"; es de suma importancia poder contar con información de los ejércitos de los países limítrofes y ser volcadas a las unidades desplegadas en la zona fronteriza, de esta manera las operaciones realizadas podrían ser más efectivas evitando amenazas transnacionales.
  Afectación: SUSTANCIALMENTE POSITIVA
- Para el indicador estratégico Nro. 2: "Capacidad de Captación de Personal Superior y Subalterno"; en lo que respecta al intercambio de Información con los ejércitos de Argentina y Brasil se considera que afecta levemente, únicamente por ser una operación visible para la Sociedad, no por el hecho de relacionarse directamente con Personal de los Ejércitos mencionados.
  Afectación LEVEMENTE POSITIVA
- Para el indicador estratégico Nro. 3: "Capacidad de Instrucción y Entrenamiento Personal"; la información recibida por parte de los Ejércitos mencionados activaría y pondría en funcionamiento mecanismos ya existentes, dándole posibilidad a los elementos del Estado Mayor de Ejército de planificar futuras operaciones, y en los niveles inferiores de realizar operaciones con mayor efectividad. No siendo necesaria instrucción previa para la misma.
  Afectación LEVEMENTE POSITIVA
- Para el indicador estratégico Nro. 4: "Capacidad de Cumplimiento de Misiones de Paz y Similares"; el hecho de tener mayor o menor información de la situación existente a la hora de realizar operaciones va a redundar únicamente en la efectividad de la misma, se considera que afecta levemente el hecho de poder contar con la misma o no, ya que los procedimientos operacionales no se modifican.
  Afectación LEVEMENTE POSITIVA
- Para el indicador estratégico Nro. 5: "Capacidad de Soporte Logístico en Actual Despliegue"; la realización de operaciones más efectivas debido a poder contar con información proveniente de los Ejércitos Argentino y Brasilero se traduciría en desplegar únicamente el personal necesario para actuar ante una amenaza identificada, evitando de este modo el despliegue de personal y medios en forma innecesaria, disminuyendo potencialmente el despliegue logístico.
  Afectación SUSTANCIALMENTE POSITIVA
- Para el indicador estratégico Nro. 6: "Capacidad Presupuestal para Funcionamiento e Inversiones de Funcionalidad Operativa"; de igual forma que para el indicador anterior, el despliegue únicamente de los medios necesarios, reduciría sensiblemente los gastos e inversiones públicas para llevar adelante la operación.
  Afectación SUSTANCIALMENTE POSITIVA

Imagen: Análisis de documentos cartográfico en Op. Frontera Segura.
Fuente: Dpto. Comunicación Institucional del Ejército.

CONCLUSIONES

El análisis del tema asignado por la metodología prospectiva a través del proyecto "Aldebarán" permitió generar un escenario estratégico probable en la cual arrojó un resultado favorable, pudiendo determinar que a corto y mediano plazo habrá un mayor fortalecimiento y consolidación del intercambio de información entre los Ejércitos de la República Argentina y República Federativa de Brasil.

El resultado del análisis evidencia que el intercambio de información entre los Ejércitos, en lo que respecta a operaciones de Frontera, es prácticamente nulo, sí se han realizado operaciones en forma conjunta principalmente con medios y personal de la Fuerza Aérea Uruguaya y la Armada Nacional, pero particularmente con el Ejército algunos ejercicios orientados al empleo de medios en las misiones operativas de paz. Esto también se debe a que el empleo de medios del Ejército en operaciones de vigilancia de Fronteras en la región es relativamente reciente, el pionero fue el Ejército Brasilero, luego el nuestro en el año 2020 y el Ejército Argentino únicamente ha empleado medios en la Frontera Norte y por períodos reducidos.

Actualmente y debido a la promulgación de la Ley de Frontera se han comenzado a allanar caminos en lo que respecta al intercambio de información, es el caso de las patrullas fluviales por el Rio Uruguay o la vigilancia del espacio aéreo con la Republica Argentina. Habiendo sido analizadas reglamentaciones de la República Federativa del Brasil encontramos que existe la voluntad de intercambio de información en pro de la vigilancia regional de fronteras, particularmente en el Proyecto SISFRON.

A mediano plazo se aprecia la voluntad política de orientar el esfuerzo y empleo de inteligencia en conjunto con autoridades de Brasil y Argentina para evitar el surgimiento de amenazas transnacionales, acorde a reuniones bilaterales llevadas a cabo entre los Ministros de Defensa de ambos países.

Habiendo sido analizada y evaluada la TEPos N°1 que posteriormente se convirtió en TEPro N° 1 debido a la evaluación obtenida por el saber colectivo podemos concluir que el análisis Prospectivo ha sido una herramienta fundamental para poder comprender la realidad en lo que respecta al intercambio de información entre los Ejércitos, pudiendo identificar que si hacemos énfasis en poder participar en ejercicios conjuntos en temáticas de frontera, participar en cursos principalmente con el Ejército de Brasil o poder acceder al Proyecto SISFRON, podemos influir en favor de nuestros intereses y de esa manera poder ser más eficientes en el accionar de nuestros medios en el cumplimiento de la vigilancia de la Frontera.

Imagen: Op. Frontera Segura.
Fuente: Dpto. Comunicación Institucional del Ejército.

Referencias Bibliográficas

C.A.R.U. (5 de diciembre de 2019). Digesto sobre el uso y aprovechamiento del Río Uruguay .
Ley 16.424. (4 de octubre de 1993). "Acuerdo para la reducción de la demanda, prevención del uso indebido y combate de la producción y trafico ilícito de estupefacientes".
Ley 17.095. (16 de mayo de 1999). "Acuerdo Bilateral Uruguay-Brasil".
Ley 18.650. (19 de febrero de 2010). "Ley Marco de Defensa Nacional".
Ley 19.677. (26 de octubre de 2018). "Autorización a las Fuerzas Armadas la realización de tareas de vigilancia y apoyo a organismos con jurisdicción y competencia en zona fronteriza".
Tratado de limites del rio de la plata y su frente marítimo. (12 de febrero de 1974).

CONFLICTO ARMADO ENTRE RUSIA Y UCRANIA

Imagen: Ilustrativa del conflicto armado entre Rusia y Ucrania.
Fuente: El Orden Mundial

El presente artículo es la continuación del trabajo presentado por el May. Juan Sbarra publicado en la Revista E.C.E.M.E. N°3 de Agosto 2024 titulado "Lecciones tácticas en el conflicto Rusia-Ucrania.

INTRODUCCIÓN

En la que por ahora es denominada "Conflicto Armado entre Rusia y Ucrania", se han sucedido desde febrero de 2022 muchos combates y batallas, en todos los ambientes y dominios que puede abarcar la guerra moderna de alta intensidad. Por su espectacularidad y simbolismo, han adquirido mayor visibilidad al público en general las batallas urbanas, pero han existido importantes enfrentamientos armados en campo abierto, bosques, islas y pequeñas localidades que por su dimensión podrían parecer irrelevantes, pero que tácticamente cobran relevancia y han tenido efectos operacionales y estratégicos. Algunos ejemplos han sido la Isla de la Serpiente, el cruce del Río Donets o la aldea de Robótyne.

Es por ésta razón que se analizarán dos batallas o combates; en un cruce de río y un asalto a una posición fortificada en campo abierto. De ése modo se pretende analizar en lo que al nivel táctico de la guerra refiere, que ha cambiado, que se mantiene vigente y que cosas en desuso han regresado del pasado, readquiriendo vigencia.

OPERACIONES DE PASAJE DE CURSOS DE AGUA.

En mayo de 2022, se sucede un cambio de enfoque en la Guerra por parte de Rusia, marcado por el abandono del territorio conquistado en al norte de Ucrania y de ésa manera hipotecando la posibilidad de conquistar Kiev y terminar rápidamente el conflicto.

Entonces el esfuerzo se concentra en la Región de Donbas y para ello era necesario cruzar el Río Donets, con el propósito de avanzar hacia la ciudad de Lysychansk, envolviendo por la retaguardia profunda a las defensas ucranianas orientadas hacia el este, con esfuerzo en impedir la conquista de las ciudades de Severodonetsk y Lysychank, separadas por el río Donets.

La zona escogida para el cruce era muy boscosa, con limitada red de caminos y estos de una calidad muy baja. Esto dificultaba los desplazamientos y la logística de la operación, si bien facilitaba el enmascaramiento de la fuerza, aunque dados

Revista ECEME

MAYOR JOSÉ MACHADO

Oficial Jefe del Arma de Infantería, actualmente Jefe de las Divisiones II y III de la D.E.IV.

Es Diplomado en Estado Mayor y Magister en Estrategia Militares Terrestre.

Prestó servicios en diferentes Unidades del Arma.

Participó en M.O.P. en la República de Haití en 2011.

PALABRAS CLAVES

GUERRA
NIVEL OPERCIONAL

los avances tecnológicos del s. XXI, demostraría no ser suficiente.

El terreno forzaba el empleo de formaciones en columna, vulnerables al fuego de artillería, con limitada capacidad de fuego hacia el frente y de poder realizar rotaciones en el esfuerzo ofensivo. La distancia entre el punto de cruce y el final de las columnas sería de entre 6 y 8 km de extensión en profundidad. La conjunción de estos factores favorecía claramente a los defensores, pero también ayudaban a los atacantes en la obtención del efecto sorpresa, por ser poco obvia la elección del punto de cruce.

Estos mantenían vigilancia sobre la margen del río, en previsión a un posible intento de cruce, pese a que ése sector era secundario, por las características enunciadas previamente. Pese a eso contaban con posiciones preparadas pero no ocupadas orientadas en ésa dirección, construidas en las alturas dominantes a unos 2 km al sur de la cortadura del curso de agua. Sabiamente no se habían posicionado en la margen del río, terreno bajo, cubierto de vegetación y con escasas rutas de repliegue y de contrataque.

A la luz de lo ejecutado por las fuerzas rusas y de los resultados, se puede deducir que el plan era "simple", organizar elementos de maniobra nivel Unidad reforzada o Gran Unidad Táctica Elemental disminuida[1], dotados de muchos medios blindados y mecanizados, con capacidad anfibia para poder vadear y/o navegar en caso de ser necesario, reforzados con Artillería y medios de Ingenieros de escalones superiores.[2] Establecer tres ejes de ataque con hasta cuatro puntos de cruce (dos para el esfuerzo principal), dominar los mismos y una vez consolidadas esas primeras líneas de alturas, realizar una explotación del éxito, sorprendiendo al enemigo antes de que movilizará reservas para bloquear y contraatacar. La Gran Unidad en reserva que realizaría la explotación sería la 90° División de Tanques de la Guardia, que estaba estacionada a unos 8 a 10 km a retaguardia, orientada al esfuerzo principal. (Quevedo, 2022)

La realidad es que la inteligencia ucraniana identificó las concentraciones de medios mientras se realizaban y desplazó hasta cinco brigadas mecanizadas, unidades separadas de artillería y Guardia Nacional, para bloquear los puntos de pasaje. El frente del asalto tenía unos 15 km de extensión, distando los puntos de cruce de entre 6 y 7 km unos de otros, permitiendo solamente el apoyo mutuo por fuego indirecto. Esta selección tan simétrica no parece ser casual u obligada por las características del curso de agua, probablemente es un intento por parte de los planificadores de aumentar el sigilo y la sorpresa en la operación, sacrificando masa en favor de la dispersión.

Ante la acumulación de medios, ya el 2 de mayo las fuerzas ucranianas reorientan los medios mencionados antes. Pero por causas que se desconocen, el plan de ataque permaneció inmutable. Ése mismo día comenzó la preparación artillera del ataque en toda la línea de 15 km, la misma duraría hasta la noche del 4 al 5 de mayo, dónde se intentó el primer cruce, en el eje de Dronivka, el cual se saldó en derrota para los atacantes, pese a haber reintentado forzar el cruce durante las jornadas del 5 y 6 de mayo, con refuerzos de la República Popular de Donetsk. (Quevedo, 2022)

Imagen: Material de ingenieros abandonado en el punto de cruce.
Fuente: Google Maps (2024).

1 En el orden de batalla ruso eran unidades de nivel de Brigada, pero por su organización y desgaste previo no podrían considerarse a ése nivel acorde a nuestra doctrina.
2 Medios de Ingenieros de la 12° Brigada Independiente de Ingenieros de la Guardia.

En tanto, más al este, en Bilohorivka, la preparación de artillería comienza en la misma noche del 4 al 5 y continúa hasta el 7 de mayo. Las fuerzas en la defensa se posicionan en las alturas que dominan el cruce, usando como puntos fuertes las explotaciones mineras a cielo abierto, situadas entre los 1.500 y 2.000 metros del punto de cruce, proporcionando dominancia de fuegos y protección a los defensores.

El cruce lo realizaron dos Grupos Tácticos de Batallón, en la noche del 7 al 8 de mayo, apoyados por artillería e ingenieros, al amparo de la oscuridad y el humo del bosque incendiado por el fuego de artillería, que fue incrementado por los fumígenos de las tareas de oscurecimiento. Primero cruzaron vehículos de combate de infantería (V.C.I.) y tanques con capacidad anfibia, para ocupar la orilla lejana y permitir los trabajos de ingenieros, (en este caso no se menciona el uso de botes), favoreciendo la movilidad, el poder de fuego y la velocidad por encima del sigilo. La oposición fue escasa y al amanecer del 8 de mayo había dos puntos de cruce tendidos y operativos, pero muy cerca uno del otro.

Al amanecer del 8 de mayo, la fuerza que cruzó el río intento explotar el éxito obtenido, dirigiéndose al Pueblo de Bilohorivka, pero fue bloqueada a dos mil metros de la cabeza de puente por posiciones de infantería. En tanto el flujo de vehículos continuaba y se produjo una aglomeración de medios en un pequeño espacio de terreno boscoso, que obligaba a permanecer cerca del camino a los vehículos.

La reacción de la artillería ucraniana no se hizo esperar, (conste que en esas fechas no estaba extendido aún el empleo masivo de drones comerciales adaptados en un rol de ataque), empleando observadores avanzados con drones dirigieron un fuego preciso sobre el punto de cruce, destruyendo los dos puentes en la tarde del mismo 8 de mayo, dejando aisladas y fijadas a las unidades rusas en un terreno desfavorable. Asimismo el fuego se enfocó en los elementos acumulados en ambas orillas del río, particularmente al sur, causando una gran destrucción de material y muchas bajas en las tropas.

Habiendo soportado en la cabeza de puente, el castigo del fuego directo e indirecto ucraniano, en la mañana del 9 de mayo se intenta un nuevo cruce en el mismo lugar, lográndose tender un puente. En apoyo a ésta operación, con la intención de liberar presión o generar dilemas al mando ucraniano, 4,5 kilómetros más al noreste, en la región de Shypylivka se realiza un intento de cruce, pero es rechazado sin lograr tender un solo puente. (Quevedo, 2022)

El 9 de mayo el mando ucraniano conocía cual era el esfuerzo e intención de las fuerzas rusas en su Área de Operaciones, orientando los esfuerzos hacia allí, incluidos el de la Fuerza Aérea. En la tarde de ése día es inutilizado el puente y las fuerzas rusas en ambas márgenes sufren pérdidas a causa del enfoque de los fuegos en su dirección. Al norte del río los escalones de retaguardia divisionarios y de las brigadas y las zonas de concentración de la reserva local son

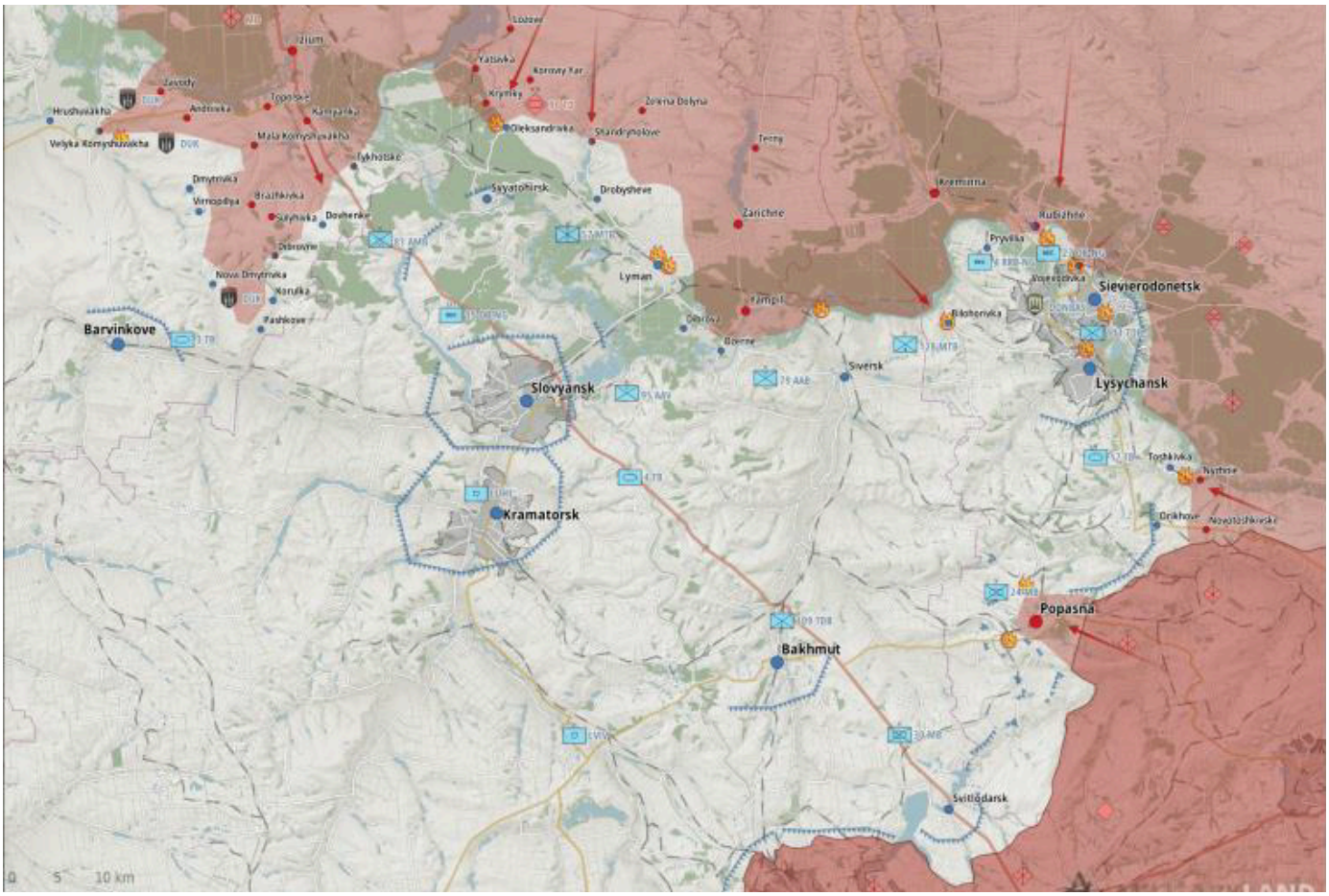

Imagen: Situación del frente al 12 de mayo de 2022.
Fuente: MilitaryLand.net.

batidas, al igual que la bolsa formada entre la defensa ucraniana y el río. Una penetración en ése flanco significaría el colapso de una línea defensiva de casi 100 km de frente y el potencial cerco de dos ciudades, de más de cien mil habitantes cada una y de unas cuatro brigadas que las defendían.

Pero lejos de terminar, la Batalla recién comenzaba, entre la noche del 9 y el día 11 se suceden los combates más encarnizados, pues las tropas de Ucrania pasan a la ofensiva para aniquilar la cabeza de puente y los asaltantes convertidos en defensores, se aferran al terreno tratando de mantener la posición hasta que lleguen refuerzos. Estos no llegan pese a los intentos continuados sobre el mismo punto de forzar el cruce, el fuego indirecto y la aviación impiden el pasaje del curso de agua. (Quevedo, 2022)

Finalmente, entre el 11 y el 12 de mayo, las tropas rusas se retiran al norte del río, empleando los vehículos con capacidad anfibia o a nado, abandonando el material, previa inutilización de los mismos.

El fracaso de esta operación tuvo el efecto inmediato de más de 400 bajas y 93 vehículos de combate de diverso tipo destruido o dañado, además de la perdida en grandes cantidades del preciado material de puentes. Eso solo en el punto de cruce en Bilohorivka, en toda la operación se estima hasta en 1.500 las bajas en tropas y 150 vehículos. Además de forzar a las fuerzas armadas de la Federación Rusa a empeñarse en una batalla urbana de gran escala en la aglomeración de Sievierodonetsk y Lysychansk, con su respectivo costo en bajas y desgaste material.

El efecto a largo plazo fue que logró mantener estabilizado el frente en la zona por más de dos años, favoreciendo a las operaciones ucranianas de otoño de 2022 en el norte del país, que permitieron la reconquista de grandes porciones de territorio.

Como lección aprendida de ésta operación, se podría rescatar el hecho de que en el Siglo XXI, lograr la sorpresa a nivel Operacional es extremadamente difícil, aunque ésta fuera una operación a nivel Táctico, su éxito hubiese tenido efectos a nivel Operacional. Esta dificultad está dada por la cantidad y calidad de sensores remotos presentes en tierra, mar, aire y espacio exterior, sumados a la observación e información proporcionadas por las personas en el terreno, que dotadas de un teléfono celular inteligente, acceso a internet y a redes sociales, pueden brindar información en tiempo real, revelando blancos y descubriendo fuerzas que en el Siglo XX hubiese sido mucho más fácil enmascarar.

Por contraparte, si bien se puede criticar la elección de un terreno muy restrictivo y canalizado para el esfuerzo principal de la operación, ésta parece ser la respuesta a la situación antes descripta, sacrificando los otros principios de las operaciones militares en beneficio de la sorpresa y la seguridad, aunque en éste caso, las medidas de seguridad tomadas, fueron insuficientes. Particularmente resalta la deficiente protección antiaérea del punto de cruce, que es uno de los aspectos doctrinales más básicos a tener en cuenta durante éste tipo de operaciones.

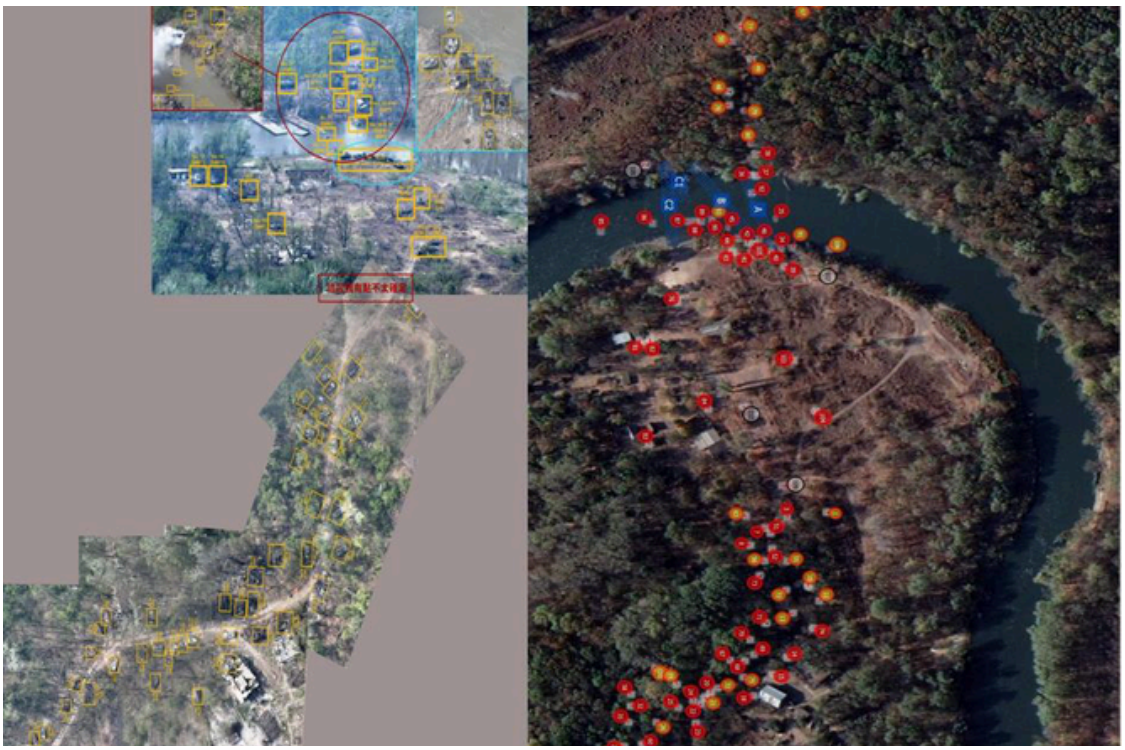

Imagen: Imagen aérea editada de la zona de Bilohorivka luego de finalizada la batalla, resaltándose los vehículos abandonados y destruidos en la cabeza de puente.
Fuente: Revista Ejércitos. (Quevedo, 2022)

Aunque el aspecto más cuestionable de ésta operación, es el empeño en forzar la ruptura desde una posición desventajosa del terreno, aun cuando todo indicaba que el esfuerzo era estéril y la mejor medida era replegar los medios a tiempo, para preservarlos. Particularmente al personal especializado, que es el más difícil de instruir y entrenar, por tanto de reemplazar a corto plazo.

El combate de Balka Uspenivska, es seleccionado por tres motivos, haberse desarrollado en un área rural, haberse empleado lo último en equipamiento y tecnología militar y por haber enfrentado a tropas equipadas y entrenadas por la O.T.A.N. contra fuerzas que empleaban doctrina del "Pacto de Varsovia", por definirlo de alguna manera simple.

Entre el 4 y 5 de junio de 2023 da comienzo una de las operaciones militares más mediatizadas y cargadas de expectativa en la historia, la "Contraofensiva Ucraniana", tanto así que hasta tenía su propio spot publicitario. Es en la madrugada de ése día que ocurren los hechos que se relatarán, aunque fueron planificados y ensayados mucho tiempo antes.

En los meses previos hubo mucha especulación en los medios de comunicación y en el ámbito académico militar sobre dónde sería el punto geográfico en que se desarrollaría la ofensiva. La preparación de las tropas ucranianas en países de la OTAN y su equipamiento con vehículos de combate y armas de apoyo de ése origen, hacían prever que se desarrollaría en un terreno que tuviera amplios campos de tiro y espacio de maniobra suficiente para desarrollar el poder de combate de grandes unidades de armas combinadas y fuertes en medios blindados.

En respuesta, Rusia fortificaba los territorios conquistados en 2022, con líneas defensivas continuas a lo largo de 150 km de frente, con hasta tres sectores defensivos sucesivos, que le daba profundidad a su dispositivo. Entre la primera línea y la segunda había hasta 30 kilómetros de distancia. En todas se establecieron densos campos minados, zanjas antitanque, líneas de dientes de dragón, alambradas, trincheras, casamatas, refugios subterráneos de hormigón, sofisticados hospitales de campaña construidos desde cero en el subsuelo y redes de túneles para interconectar las posiciones y abastecerlas fuera de la vista del enemigo, entre otras obras de organización del terreno.

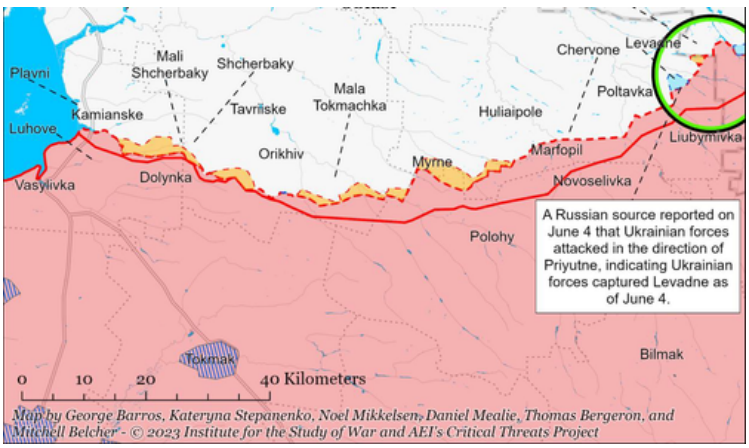

Imagen: Extracto de un mapa del sector del frente en el que se encuentra enmarcado el Asalto a Robotyne, la fecha del mismo es del día del comienzo de las Ops. Ofensivas ucranianas.
Fuente: Revista Ejércitos. (Quevedo, 2022)

A éste complejo dispositivo defensivo en apariencia estático[3] se le dio el nombre informal de "Línea Surovikin" en honor al Comandante ruso de ése Teatro de Operaciones. Tal dispositivo defensivo recordaba a la defesa rusa de Kursk en 1943. (Nor Sevan. Noticias de la comunidad, Armenia, Artsaj, el Cáucaso y el Mundo., 2023)

El 1 de mayo de 2023 la inteligencia británica advertía sobre las capacidades de las obras defensivas rusas expresando entre otros conceptos lo siguiente:

> **"Rusia ha construido algunos de los sistemas más extensos de obras defensivas militares vistos en cualquier parte del mundo durante muchas décadas".**

Los resultados de la ofensiva ucraniana confirmarían con creces la certeza de ésos dichos. (Proto, 2023)

El 4 de junio dio inicio la ofensiva de primavera del Ejército ucraniano, buscando tomar la Iniciativa Estratégica y recuperar territorio ocupado. Tras ataques de distracción en flancos, lanzaron su ataque principal la noche del 7 de junio.

Una Brigada Mecanizada fue asignada para romper la primera línea defensiva rusa en el sector de Robotyne, pero asaltando las posiciones del flanco este de la localidad. Su plan implicaba dos Equipos de Combate en base a subunidades mecanizadas, equipadas con Vehículos de Combate de Infantería (VCI) del modelo M2 Bradley en diversas de sus variantes, reforzadas con una Sección de Tanques equipada con Leopard 2 y Vehículos de Combate de Ingenieros. La progresión se desarrolló al amparo de la noche y avanzando en columna, precedidos por los elementos de ingenieros para brechar los obstáculos de la defensa rusa.

Aprovechando la superioridad en observación y adquisición de blancos brindada por las ópticas del material blindado, se infiltraron de noche y a cubierto de densas líneas de árboles, que los ocultaban de la observación del enemigo. Sin embargo, al acercarse a la carretera T0803, el primer Equipo de

3 En la práctica se ejecutó una Operación de Defensa Activa.

Combate encontró un campo minado no detectado, posiblemente diseminado remotamente empleando artillería, vehículos lanza minas o incluso drones, poco tiempo antes del inicio del avance ucraniano.

Las explosiones alertaron a los defensores y atrajeron fuego de misiles antitanque (A/T), demostrando la efectividad del emplazamiento avanzado de equipos A/T, los que estaban operados por elementos de las Fuerzas Especiales rusas, cumpliendo un rol inusual, con la tarea de adelantar la línea de contacto de la defensa.

Una vez que la defensa tomó contacto con los primeros elementos asaltantes, inició acciones de reconocimiento, probablemente con drones equipados con cámaras térmicas o de visión nocturna y lograron identificar al segundo Equipo de Combate que estaba aún a cubierto, más a retaguardia, batiéndolo con fuego de Artillería.

Pese a esto, entre ambos elementos empeñados, logran abrir brecha en el campo minado y cruzar la carretera T0803 hacia el sur, estableciendo una Base de Apoyo de Fuego, desde donde batieron a las posiciones defensivas rusas, permitiendo que la Reserva de la Unidad asaltara y conquistara la Posición Defensiva N°2.

Durante la mañana la tercera Posición defensiva es conquistada, se presupone por medios del Batallón en Reserva de la misma Brigada ucraniana a la que pertenecía la Unidad que había atacado durante la noche. (Moyano, 2023)

Pero las reservas rusas contraatacan con medios de valor Fuerza de Tarea Mecanizada (probablemente un BTG[4]) y los combates se prolongan durante toda la jornada, existiendo dos versiones diferentes sobre el desenlace final de ése día; una en que son desalojadas las fuerzas ucraniana s de las posiciones conquistadas en la madrugada. Y otra en que los defensores reconquistan la Posición Defensiva N° 3, pero las fuerzas ucranianas mantienen una posición en las alturas que dominan por el sur la ruta T0803 y la ruta T0815, la vía ferroviaria paralela a la misma y el pueblo de Mala Tokmachka, el cual servía como zona de reunión y punto de partida de las acciones ofensivas de las unidades ucranianas.

Tácticamente el Ejército de Ucrania logra una victoria parcial, al aferrase a un punto crítico que dominaba a la primera línea de defensas rusa, que eran en esencia Puestos Avanzados Generales de la Posición Defensiva Principal, pero a nivel Operacional la maniobra es un fracaso, puesto que no se cumplió con el objetivo de abrir una brecha que permitiera el ingreso de segundos escalones de ataque dirigidos hacia las posiciones principales de la defensa.

Si bien no conocemos con exactitud los objetivos del ataque ucraniano, se pueden deducir a través del estudio del terreno y de la apreciación de la cantidad y tipo de medios empleados por los atacantes. Suponemos que el elemento en Primer Escalón tenía por objetivo conquistar al menos una de las tres posiciones defensivas a nivel Compañía, pero debido a los

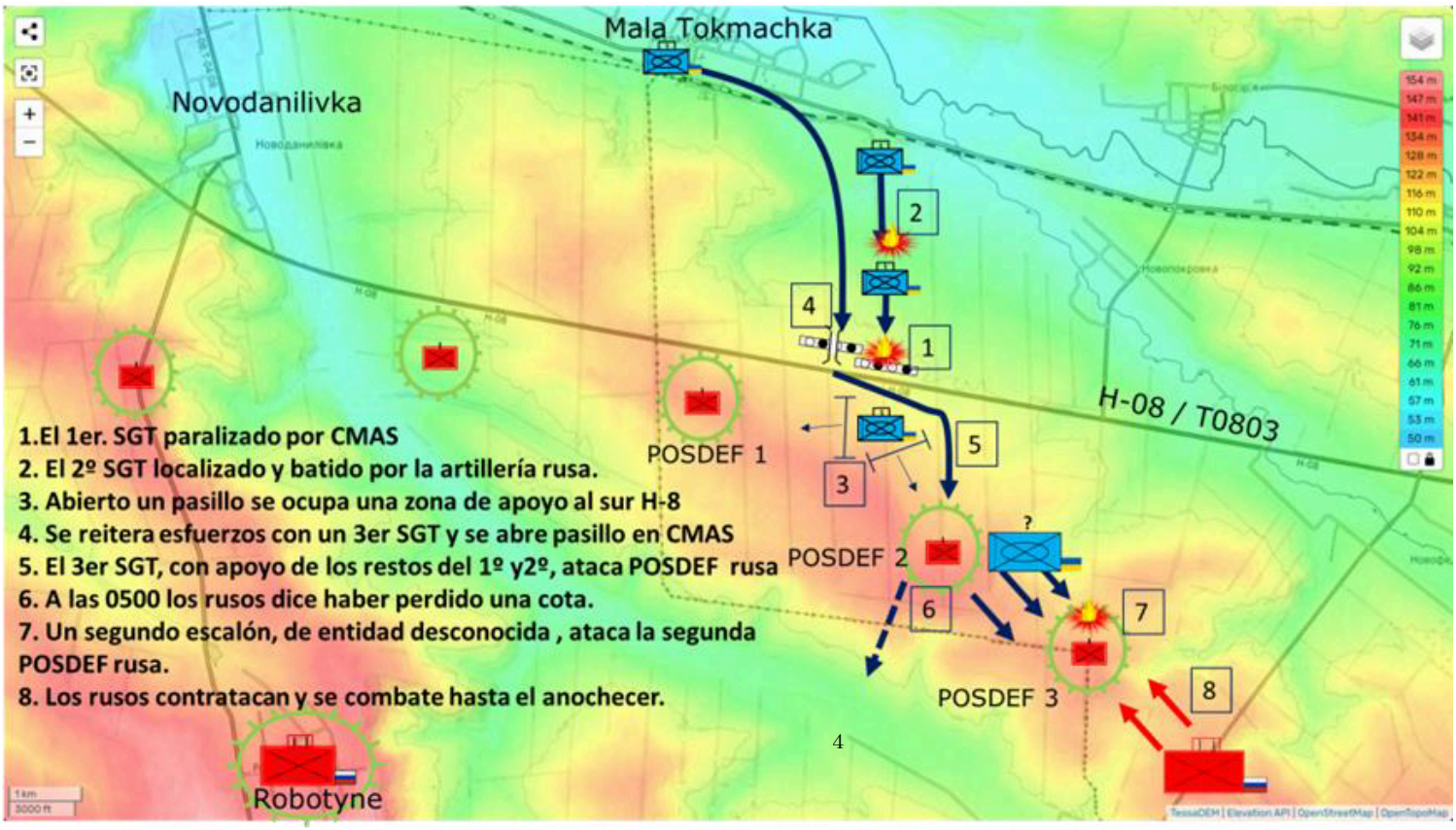

Imagen: Croquis del desarrollo de las acciones:
Fuente: Extraído del Artículo "El combate de las lomas de Balka Uspenivska" de la Revista Ejércitos (Moyano,2023)

4 BTG: Grupo Táctico de Batallón por sus siglas en inglés.

medios técnicamente superiores y los apoyos al combate disponibles, pudieran tener por objetivo incluso dos de las tres posiciones, siendo la segunda sub unidad atacante la responsable de asaltar la tercera posición, a favor de una base de apoyo de fuego establecida en las posiciones uno y dos.

Explotando luego ése éxito inicial con otra Unidad de tipo Fuerza de Tarea fuerte en blindados, cuyo objetivo más lógico sería la posición defensiva en Robotyne, expuesta desde el flanco Este por la maniobra ofensiva realizada. La conquista de Robotyne permitiría desarrollar un ataque hacia el Sur, en dirección a Tokmak, una localidad muy importante y que articulaba un importante sector de la defensa rusa y su caída amenazaba la integridad de toda la defensa en dirección a Crimea.

Si bien la operación analizada era de nivel Táctico, estaba enmarcada en una operación de nivel Operacional, y su fracaso o éxito parcial, impidió la conquista de al menos un Objetivo Operacional, es previsible asumir que éste hecho afectó negativamente a la sincronización y al ritmo de las operaciones planificadas.

Luego del análisis, se puede determinar que el asalto fracasa principalmente por el contacto prematuro con obstáculos no identificados en el reconocimiento previo y que estaban cubiertos por el fuego desde posiciones tampoco reveladas en el reconocimiento. El desgaste y desorganización infligida en la zona de obstáculos y el consecuente prematuro empleo de la Reserva, impiden la consolidación de los objetivos antes de la reacción de la Reserva rusa. Es este contraataque y el posterior combate hasta la caída de la noche, lo que termina cerrando la posibilidad de realizar el ataque a Robotyne, donde también es previsible que se hubiese reorientado el esfuerzo de la defensa para atender a la nueva amenaza.

Es importante destacar que son los elementos artificiales agregados al entorno rural antes de la guerra, los que condicionan las maniobras defensivas y ofensivas, pero en éste caso principalmente a las últimas.

A ése respecto, es la orientación de las plantaciones de árboles, de las carreteras, la vía del tren y los pequeños centros urbanos aledaños a la posición defensiva los que determinan la ubicación de los ejes de progresión, posiciones de ataque y las zonas de reunión previas, aspectos que pueden pasarse por alto en la visión macro de la planificación al nivel de la Gran Unidad, pero que afectan drásticamente la planificación y ejecución de la sub unidad del esfuerzo principal cuya misión es conquistar el Punto Decisivo, del que depende el éxito de toda la maniobra.

CONCLUSIONES.

Como conclusión general de éste análisis de las batallas en Ucrania, se puede observar que, pese a las características singulares de cada tipo de combate, existen lecciones generales aplicables a la guerra moderna, tanto en el ámbito táctico, como en el operacional y estratégico.

Respecto a las Operaciones de Pasaje de Cursos de Agua, la fallida operación de cruce del Río Donets por parte de Rusia es un ejemplo categórico de cómo los avances tecnológicos del siglo XXI han transformado la guerra moderna. La capacidad de observación y adquisición de blancos a nivel táctico, mediante drones y otros sensores remotos avanzados, hizo que alcanzar y mantener la sorpresa fuera sumamente difícil.

No puede pasarse por alto el hecho de que en apariencia la fuerza de cruce carecía o estaba muy escasamente dotada de armas antiaéreas, lo cual está previsto en su doctrina. Esto, sumado a la mala o al menos cuestionable elección del terreno, que obligaba a adoptar formaciones poco dispersas y canalizadas, agravado todo esto por la falta de flexibilidad del mando para adaptarse a una situación de desgaste elevado de los medios empleados, resultó en el fracaso de la operación.

De esta batalla se desprende que, aunque las operaciones de cruce de ríos siguen siendo una tarea critica en la maniobra terrestre, el planeamiento debe tener en cuenta la capacidad de reacción casi inmediata del enemigo, especialmente en terrenos tan restrictivos y con líneas de comunicaciones largas y vulnerables al cada vez más amplio y profundo radio de acción de la observación y el control de fuego, con los que cuentan hasta los más bajos niveles de fracción.

En cuanto a las operaciones en zonas rurales, el combate en Balka Uspenivska durante la contraofensiva ucraniana ilustra los desafíos de llevar a cabo operaciones ofensivas en terrenos densamente fortificados. A pesar de la superioridad tecnológica ucraniana, representada por el uso de vehículos modernos como los VCI Bradley y los Tanques Leopard 2, la presencia de campos minados, zanjas anti tanque, fortificaciones bien organizadas en frente y profundidad, dotadas de defensores bien preparados y motivados, ralentizó y, en algunos casos, bloqueó a los atacantes.

La ofensiva ucraniana no logró su objetivo principal de romper completamente la primera línea defensiva rusa, demostrando que las líneas de fortificaciones tradicionales y rígidas, cuando están adecuadamente preparadas y defendidas, pueden ser una barrera formidable incluso para fuerzas equipadas con tecnología avanzada. Además, la aplicación de una Defensa Activa, a través del empleo de

constantes contraataques rusos, complementado con el uso de drones y artillería, muestra que el ritmo de las batallas defensivas en zonas rurales puede ser mucho más dinámico de lo esperado para un entorno aparentemente favorable para la maniobra ofensiva.

La ofensiva ucraniana no logró su objetivo principal de romper completamente la primera línea defensiva rusa, demostrando que las líneas de fortificaciones tradicionales y rígidas, cuando están adecuadamente preparadas y defendidas, pueden ser una barrera formidable incluso para fuerzas equipadas con tecnología avanzada. Además, la aplicación de una Defensa Activa, a través del empleo de constantes contraataques rusos, complementado con el uso de drones y artillería, muestra que el ritmo de las batallas defensivas en zonas rurales puede ser mucho más dinámico de lo esperado para un entorno aparentemente favorable para la maniobra ofensiva.

Hay lecciones comunes que se pueden extrapolar de todas estas operaciones incluyendo los que se suceden en áreas urbanizadas. En primer lugar, la importancia de la integración tecnológica en la guerra moderna es innegable. Drones de reconocimiento, munición de artillería guiada por GPS, y la capacidad de observación en tiempo real mediante satélites y otras tecnologías avanzadas, han reducido drásticamente la posibilidad de obtener una sorpresa táctica y, en muchos casos, han definido el resultado de los combates. El concepto clásico de sorpresa ha sido profundamente afectado, lo que obliga a los planificadores militares a buscar nuevas maneras de ocultar sus intenciones o, al menos, a mitigar la capacidad del enemigo para detectar y reaccionar.

En segundo lugar, la capacidad de adaptación de los mandos ha sido un factor determinante en todos los casos analizados. Tanto las fuerzas rusas como las ucranianas han demostrado flexibilidad a lo largo de la guerra, ajustando sus tácticas y doctrinas según las lecciones aprendidas en el campo de batalla. Sin embargo, los errores persistentes, como la insistencia rusa en forzar un cruce de río en condiciones desfavorables o la obstinación ucraniana en romper líneas defensivas sin una adecuada evaluación de los avances iniciales o del grado de resistencia encontrado, demuestran que en la guerra moderna, la rigidez doctrinal sigue siendo un grave defecto.

Por último, el alto costo en bajas de oficiales superiores en ambos bandos refleja una cultura de liderazgo que promueve la presencia de los comandantes en la primera línea de batalla. Si bien esto puede inspirar a las tropas y mejorar la toma rápida de decisiones, también expone a los mandos a un riesgo innecesario, lo que tuvo como resultado la pérdida de varios oficiales generales y de comandantes de tropas importantes. Esta tendencia parece haberse corregido con el tiempo, al menos parcialmente, pero sigue siendo un aspecto a considerar en futuros conflictos, donde la importancia de preservar los cuadros de mando es vital para mantener la cohesión y la eficacia operativa.

Queda en evidencia que la capacidad para aprender de los errores y ajustar el enfoque en tiempo real es lo que, en última instancia, puede marcar la diferencia en el resultado final de las operaciones.

Referencias Bibliográficas

Bailey, R., Hird, K., Stepanenko, K., Wolkov, N., & Kagan, F. W. (5 de junio de 2023). www.understandingwar.org.
Cerezo, M. d. (23 de febrero de 2023). rtve.es.
Deep State Map. (5 de mayo de 2022). www.deepstatemap.live.
Google Maps. (10 de agosto de 2024). www.google.com.
Moyano, F. J. (10 de julio de 2023). "*El combate de las lomas de Balka Uspenivska*". Revista Ejércitos, S/P.
Moyano, F. J. (20 de diciembre de 2023). "*La guerra en Ucrania y las batallas en zona urbana*". Revista Ejércitos.
Nor Sevan. Noticias de la comunidad, Armenia, Artsaj, el Cáucaso y el Mundo. (21 de junio de 2023). norsevan.com.
Proto, L. (15 de junio de 2023). "*Línea Surovikin*". elconfidencial.com.
Quevedo, G. M. (22 de mayo de 2022). "*Desastre en Bilohorivka. Los Puentes de Mayo*". Revista Ejércitos.
Stewart, W. (29 de marzo de 2022). www.dailymail.co.uk.

Imagen: Gral. DIvisión Pedro Sicco.
Fuente: C.G.E. - Departamento de Estudios Históricos

GENERAL DE DIVISIÓN don PEDRO SICCO: Estratega y forjador de la enseñanza superior en el Ejército Nacional

Este artículo es dedicado al General de División don. Pedro Sicco, actor clave en el proceso de capacitación de los Oficiales del Ejército. A través de esta contribución, se busca destacar el papel de Sicco como impulsor estratégico de la enseñanza superior militar, desde las más altas responsabilidades del Ejército y a la vez con su experiencia como docente para formar a los futuros conductores del Ejército Nacional y sentar las bases de lo que hoy constituye la E.C.E.M.E.

Un líder forjado en el estudio y la experiencia.

El General de División don Pedro Sicco nació en la ciudad de Montevideo el 10 de marzo de 1888, hijo de don Felipe Sicco y doña Magdalena Peluffo. Ingresó a la Academia General Militar en 1905, egresando en 1909 como Alférez del arma de Artillería. En 1923 contrajo matrimonio con la señora Cira Fontana, con quien tuvo cuatro hijos.

A lo largo de su carrera, reflejó una combinación ejemplar de compromiso profesional, formación académica y vocación por la enseñanza. Fue ascendiendo por méritos, obteniendo destacadas calificaciones en concursos y cursos de perfeccionamiento. Entre los hitos formativos de su trayectoria se destacan sus estudios en la Escuela Superior de Guerra de Francia, a donde fue enviado en 1923, convirtiéndose en el primer Oficial del Ejército Nacional en obtener el Curso de Estado Mayor. En 1945, integró la Misión Militar a los Estados Unidos, donde obtuvo los diplomas de Estado Mayor y de Instrucción Superior en la Command and General Staff School de Fort Leavenworth (Kansas City). Esta instancia completó su formación estratégica internacional recibida en Francia, orientada por las lecciones doctrinarias de la Primera Guerra Mundial, con una visión moderna basada en la experiencia aliada en la Segunda Guerra Mundial, reflejando el interés institucional por actualizar la doctrina nacional a los nuevos desafíos operacionales del mundo de posguerra.

A su vez, y en paralelo a sus funciones de mando, desarrolló una intensa labor docente en la Escuela Militar, dictando

Revista ECEME

MAYOR MAXIMILIANO VALETTA

Oficial del Arma de Artillería, actualmente alumno del Curso de Estado Mayor.

Licenciado en Ciencias Militares.

Prestó servicios en diferentes Unidades del Arma.

Participó en M.O.P. en la República de Haití.

PALABRAS CLAVES

HISTORIA
ENSEÑANZA MILITAR.
DOCTRINA

cátedras de Fortificación de Campaña, Táctica, Estado Mayor y Puente del Momento. Su compromiso con la enseñanza se reflejó tanto en el aula como en las estructuras de conducción educativa, desde donde impulsó iniciativas fundamentales para la profesionalización de los Oficiales.

Esta vocación por el perfeccionamiento doctrinario y la formación sistemática lo llevó, hacia fines de la década de 1920, a impulsar una de las iniciativas más trascendentes de su carrera: la creación de un curso destinado a preparar a los futuros oficiales de Estado Mayor.

El nacimiento de una visión: el Curso de Informaciones de Estado Mayor (1928)

En 1928, mientras se desempeñaba como 2º Comandante de la Escuela Militar, el entonces Teniente Coronel don Pedro Sicco impulsó la creación del Curso de Informaciones de Estado Mayor, aprobado por resolución del Poder Ejecutivo el 27 de marzo de ese año. El curso fue dictado en la sede de la propia Escuela Militar y dependía directamente del Estado Mayor del Ejército.

Según consta en los registros (Escuela de Comando y Estado Mayor del Ejército, s.f.), el curso tenía por finalidad "proporcionar a los Oficiales de las distintas armas los conocimientos generales más indispensables al Oficial de Estado Mayor, y complementar la instrucción militar superior, a fin de que más tarde puedan ejercer el mando de las mayores Unidades de su arma o iniciar estudios en los cursos regulares de una Escuela de Guerra" (Orden General Nº 3671).

Sicco, designado como instructor principal del curso, aportó su experiencia profesional y académica, incluyendo los estudios realizados en la Escuela Superior de Guerra de Francia. Esta primera iniciativa de formación doctrinaria sistemática representó una señal temprana de su compromiso con la profesionalización de la enseñanza militar.

El período que siguió a la creación del curso mostró una continuidad clara en su protagonismo dentro del ámbito educativo militar. La etapa comprendida entre 1927 y 1932 sería clave para cimentar el modelo formativo que tiempo después desde la Inspección General del Ejército, consolidaría esa visión a través de la institucionalización de la Escuela de Estado Mayor (actual I.M.E.S.) y la estructuración de un sistema con proyección permanente.

Imagen: Gral. DIvisión Pedro Sicco.
Fuente: C.G.E. - Departamento de Estudios Históricos

De la dirección académica al impulso institucional.

Tras haber impulsado y dirigido los primeros cursos de formación de Estado Mayor entre 1928 y 1930, el entonces Teniente Coronel don Pedro Sicco continuó desempeñando un papel clave en su consolidación académica e institucional. En 1929 fue designado Director del Curso Preparatorio de Servicio de Estado Mayor, que a partir de 1930 pasó a dictarse en el Cuartel del Regimiento de Artillería Montada Nº 1, unidad en la que Sicco asumió simultáneamente como Jefe de Regimiento. Esta función dual fortaleció su perfil como Jefe de Unidad Básica y referente académico, en una etapa donde comenzaba a delinearse una concepción estructurada de la enseñanza profesional. El curso, de dos años de duración, tenía como objetivo "dar a los

Oficiales los conocimientos necesarios para poder colaborar eficazmente en las difíciles tareas del Comando".

En 1932 se crea la Escuela de Estado Mayor (I.M.E.S.), el curso, ahora Escuela, dejó de depender del Estado Mayor del Ejército y pasó a estar bajo la órbita del Inspector General del Ejército. Aunque no se cuenta con registros específicos que acrediten su participación directa en esta etapa de reorganización, es razonable considerar que, en su calidad de Director y principal instructor, se encontraba vinculado a los procesos que condujeron a la transformación del curso en Escuela. Su experiencia previa como creador, instructor y director de los cursos fundacionales representa un antecedente doctrinario relevante que permitió sentar las bases para la posterior consolidación del sistema educativo del Ejército (Legajo personal del Gral. de División don Pedro Sicco, s.f.).

En 1934, durante su gestión como Director, la Escuela adoptó el nombre de Escuela Superior de Guerra, consolidando su perfil como centro de formación avanzada. Al año siguiente, en 1935, el curso fue rebautizado como Curso de Especialización o de Estado Mayor, con una nueva estructura dividida en dos años lectivos, lo que representó un salto cualitativo en los contenidos y exigencias del proceso formativo. Estos cambios reflejan el liderazgo sostenido de Sicco en el desarrollo doctrinario, así como su capacidad de proyectar mejoras estructurales en el sistema de enseñanza.

En este proceso de consolidación, cabe destacar un episodio complejo. En 1933, Sicco asumió simultáneamente la dirección de la Escuela de Estado Mayor (I.M.E.S.) y de la Escuela Militar de Aplicación, unificadas momentáneamente bajo su liderazgo. Dicha fusión se ajustaba plenamente al modelo pedagógico que él defendía, fue concebida como una oportunidad para integrar coherentemente los niveles del ciclo formativo del Oficial. Sin embargo, divergencias doctrinarias con el alto mando, en particular con el Inspector General del Ejército, General Gomeza, generaron tensiones que derivaron en su renuncia. Este episodio ilustra su convicción sobre la necesidad de articular la enseñanza profesional bajo criterios doctrinarios comunes, ajustados a las condiciones nacionales y orientados por una visión de largo plazo.

Imagen: Gral. DIvisión Pedro Sicco.
Fuente: C.G.E./Dpto EE.HH.

Al ascender a General, Sicco dejó la conducción de la Escuela en manos del Teniente Coronel don Cipriano Olivera, quien había integrado la primera promoción del "Curso de Informaciones de Estado Mayor".

Proyección doctrinaria y legado institucional.

En 1947, el General don Pedro Sicco ocupaba el cargo de Inspector General del Ejército, desde el cual promovió y respaldó la reestructuración llevada a cabo por el General don Edgardo Ubaldo Genta. Fruto de este proceso, el 2 de julio de 1948 se creó la Escuela de Estado Mayor (E.E.M.) mediante el Decreto del Poder Ejecutivo Nº 11.881, firmado por el Presidente de la República Dr. Luis Batlle Berres, en el marco de la aprobación del nuevo Reglamento para el I.M.E.S. A partir de ese momento, el Curso de Especialización o de Estado Mayor pasó a dictarse bajo la órbita de la nueva Escuela, marcando un punto de inflexión en el sistema de perfeccionamiento profesional. El rol de Sicco en esta etapa fue el de un articulador estratégico, que comprendió la necesidad de modernizar la formación superior sin perder continuidad con las bases doctrinarias que él mismo había contribuido a consolidar.

Actualmente, la E.C.E.M.E. constituye la expresión institucional del sistema de enseñanza superior que el General Sicco contribuyó a consolidar. Según el Reglamento de Organización y Funcionamiento del I.M.E.S., aprobado por el Decreto Nº 439/022, la E.C.E.M.E. tiene por misión desarrollar el curso de Capacitación y Perfeccionamiento de Jefes del Cuerpo Comando y Cuerpo de Servicios, el Curso de Estado Mayor, y el Curso de Capacitación a Distancia para Capitanes. Su finalidad comprende la capacitación de Jefes para desempeñarse en los distintos escalones tácticos y administrativos del Ejército en tiempos de paz, crisis o conflicto armado; la formación de Oficiales de Estado Mayor como asesores de los Comandos Estratégicos, Tácticos y Administrativos; y la iniciación de los alumnos en el estudio de los problemas de Seguridad y Defensa con énfasis en la planificación estratégica de estructuras orgánicas, administrativas y operativas. Esta misión reafirma el valor del pensamiento doctrinario y educativo impulsado por Sicco, proyectado hoy en una institución que combina continuidad con visión de futuro y modernización al servicio del perfeccionamiento profesional del Oficial del siglo XXI.

La preocupación del General don Pedro Sicco por construir una doctrina nacional no se limitó al ámbito de la enseñanza formal. A lo largo de su carrera, desarrolló una intensa actividad intelectual, convencido de que el pensamiento estratégico debía formar parte del acervo profesional del oficial. En 1952, publicó su obra Artigas a la luz del arte de la guerra (Sicco, 1952), editada por el Centro Militar, en la que analiza la acción militar del General don José Gervasio Artigas desde una perspectiva doctrinaria, estructurada sobre los principios del arte operacional y la conducción estratégica. La obra refleja una visión madura, fruto de años de estudio, docencia y responsabilidad en el diseño del sistema de enseñanza profesional del Ejército.

En este trabajo, Sicco propone una interpretación de la campaña artiguista que trasciende el relato histórico tradicional, subrayando aspectos como la economía de fuerzas, la iniciativa, la concentración del esfuerzo y la unidad de conducción. A través de este análisis, procura demostrar la validez universal de los principios militares y, al mismo tiempo, fortalecer una identidad doctrinaria nacional enraizada en la experiencia artiguista. Su enfoque revela una intención pedagógica clara: mostrar que los fundamentos estratégicos no son ajenos a nuestra historia, sino que están presentes en ella y deben ser comprendidos con criterio técnico.

Además de su obra publicada, Sicco integró comisiones claves para la revisión de reglamentos tácticos, elaboró propuestas para la reorganización del Estado Mayor del Ejército y participó activamente en misiones de estudio y representación internacional. Su actuación combinó visión, rigor y compromiso con el perfeccionamiento permanente de la institución. Por ello, puede afirmarse que su legado excede largamente su papel como instructor o director: fue un arquitecto de pensamiento, un referente doctrinario y un impulsor de la profesionalización militar en todos sus niveles.

La E.C.E.M.E., heredera de aquel primer curso que Sicco ayudó a gestar, representa hoy la continuidad institucional de una visión estratégica sobre la enseñanza superior militar. Su evolución refleja los principios impulsados por Sicco en las primeras décadas del siglo XX: una formación profesional rigurosa, doctrinariamente fundamentada y orientada a las exigencias del mando moderno.

La trayectoria del General de División don Pedro Sicco se inscribe entre las más relevantes del proceso de profesionalización del Ejército Nacional. Desde su temprana participación en la docencia militar hasta su decisiva actuación estratégica como Inspector General del Ejército, su legado combina visión estratégica,

compromiso institucional y una profunda vocación pedagógica. Supo concebir la enseñanza como un instrumento fundamental para la cohesión, la eficacia operativa y la construcción de una doctrina propia, ajustada a la realidad nacional.

Impulsor del Curso de Informaciones de Estado Mayor en 1928, formador de generaciones de Oficiales e intelectual militar, Sicco dejó una huella indeleble en el desarrollo del sistema de enseñanza profesional. Su pensamiento no sólo consolidó estructuras, sino que también proyectó una cultura de reflexión estratégica que aún hoy constituye un pilar del accionar del Ejército.

Al rendir homenaje a su figura, la E.C.E.M.E. reconoce en Pedro Sicco no solo a un director o reformador, sino a uno de sus verdaderos precursores. Su vida, su obra y su visión institucional siguen vigentes en la misión formativa que se asume cada año con nuevas generaciones de Oficiales comprometidos con la Defensa Nacional, el estudio riguroso y la excelencia profesional.

Agradecimientos.

Este artículo no habría sido posible sin el valioso apoyo de diversas instituciones y personas que contribuyeron con documentación relevante. Expresamos nuestro profundo agradecimiento al Dpto. de EE.HH. del E.M.E. y a la Fundación "General de División Pedro Sicco" por facilitar el acceso a materiales fotográfico y biográficos, a la Biblioteca Social del Centro Militar por su colaboración en la consulta de fuentes documentales, y al Licenciado Enrique Bordagorri por sus aportes.

Imagen: Gral. División Pedro Sicco.
Fuente: C.G.E./Dpto EE.HH.

Referencias Bibliográficas

Del Pino Menck, A., & Bordagorri, E. (2018). Centenario Instituto Militar de las Armas y Especialidades.
Escuela de Comando y Estado Mayor del Ejército. (s.f.). I.M.E.S. https://www.imes.edu.uy/escuela_comando_y_estado_mayor.html
Legajo personal del Gral. de División don Pedro Sicco. (s.f.). Departamento de Estudios Históricos.
Sicco, P. (1952). Artigas a la luz del arte de la guerra. Centro Militar.

Revista ECEME

Carrera “Profesor Rama”. Actividad física de camaradería y cierre del año en la Rambla de Montevideo.
NOV. 2024

Ceremonia de clausura de cursos.
NOV. 2024

Fiesta social.
NOV. 2024

Revista ECEME

Ceremonia de ascenso
I.M.E.S.
JUN. 2025.

Ejercicio Táctico
C.C.P.JJ.
JUL. 2025.

Visita al Ejercito del Brasil
SET 2025

Revista ECEME

T.A.F. - Tiro de Arma Corta
SET 2025

Ejercicio Módulo Conjunto
NOV. 2025

Maniobra de Cartas
NOV. 2025

Escuela de Comando y Estado Mayor del Ejército

Revista ECEME

MONTEVIDEO / URUGUAY
http://www.imes.edu.uy/escuela_comando_y_estado_mayor.html