TRABAJO FINAL INTEGRADOR

TEMA:

LOS CONFLICTOS BÉLICOS Y LA GESTIÓN DE LA INFORMACIÓN

TÍTULO:

OPERACIONES DE INFORMACIÓN EN EL CONFLICTO DE CRIMEA EN 2014

AUTOR: MAYOR (EA) JUAN ANTONIO CABRIGNAC

TUTOR: GENERAL DE DIVISIÓN (EA) GUSTAVO JORGE LUIS MOTTA

Año 2023

Resumen

El conflicto de Crimea comenzó a finales de 2013, por una serie de protestas en Ucrania conocidas como Euromaidán, en respuesta a la decisión del presidente ucraniano, Viktor Yanukovich, de no firmar el acuerdo de asociación con la Unión Europea. Estos reclamos fueron impulsados por el deseo de un mayor acercamiento a Occidente y una mayor independencia de la influencia rusa.

Ante la destitución del presidente, el parlamento tomó el control del país, Rusia no reconoció al nuevo Gobierno como una autoridad legítima y declaró que lo ocurrido fue un golpe de estado. Los residentes del sureste de Ucrania se manifestaron en contra del nuevo Gobierno de Kiev, incitando a una resistencia y realizando un referéndum sobre el estatus político de Crimea. Finalmente, se produjo una intervención militar, donde las fuerzas armadas rusas se desplegaron en la península, con el objetivo de garantizar la integridad de los ucranianos prorrusos habitantes de Crimea. El 17 de mayo de 2014, fue proclamada la independencia de la República de Crimea, al día siguiente fue aprobada la adhesión de Crimea a la Federación de Rusia.

Durante el conflicto, se llevaron a cabo diversas operaciones de información con el objetivo de influir en la opinión pública y moldear la percepción del conflicto, contribuyendo a la polarización de la opinión pública y a la formación de percepciones sesgadas sobre el enfrentamiento. A través del análisis de este conflicto se aprecia la trascendencia estratégica de las operaciones de información en los conflictos modernos, donde la batalla por la narrativa y la opinión pública desempeña un papel clave en el logro de los objetivos impuestos.

La presente investigación buscará determinar si las operaciones de información ejecutadas por las fuerzas de la Federación de Rusia, durante el conflicto con Crimea, contribuyeron al cumplimiento de los objetivos operacionales.

Palabras Clave

Operaciones de Información, Crimea, Influencia, Gestión

Índice

Introducción

A lo largo de la historia, a causa de la incorporación de nuevas tecnologías, armamentos y doctrinas, la forma de realizar la guerra siempre ha estado en constante cambio. Según Makotczenko (2019), en los países Occidentales se identifican cuatro generaciones: la guerra de masas, el predominio del fuego, la guerra relámpago y la guerra del débil contra el fuerte. Por otro lado, los países orientales no tienen en cuenta esta clasificación, consideran que solo hay dos formas de ejecutar la guerra, la lineal y la no lineal. Este último concepto considera que el esfuerzo principal debe centrarse en la sublevación de la población a través de la influencia de los medios de comunicación social (MCS), las fuerzas especiales, las operaciones cibernéticas y las operaciones de información (OI), por lo cual las fuerzas regulares solo se utilizarán para consolidar los objetivos y finalizar el conflicto (p. 20).

La constante evolución del ambiente operacional ha generado que los conductores precisen de nuevas tecnologías para asegurar y gestionar el flujo de información que se genera. Los amplios espacios entre sus fuerzas los ha obligado a disponer de nuevos dispositivos para adquirir una correcta apreciación de la situación, permitiéndoles lograr una percepción fiel de la realidad. De este modo, su ciclo de toma de decisiones ha incrementado su dependencia de las nuevas tecnologías de la información y las comunicaciones (TIC). Esto ha producido una revolución del pensamiento militar generando un nuevo paradigma que determina que para conducir y ganar la guerra es necesario lograr el dominio de la información (Gómez Arriagada, 2015, p. 47).

Las Fuerzas Armadas de la Nación Argentina, tanto en el ámbito específico como en el conjunto, no han desarrollado doctrina relacionada con las OI. Bilibio (2017, p. 4) considera que es necesario determinar cuáles son los conceptos centrales de las OI, sus principales capacidades, su finalidad, su alcance, la estructura orgánica necesaria para su desarrollo, su método de planeamiento y sus áreas de acción, para poder sentar las bases que permitan elaborar doctrina de OI propia.

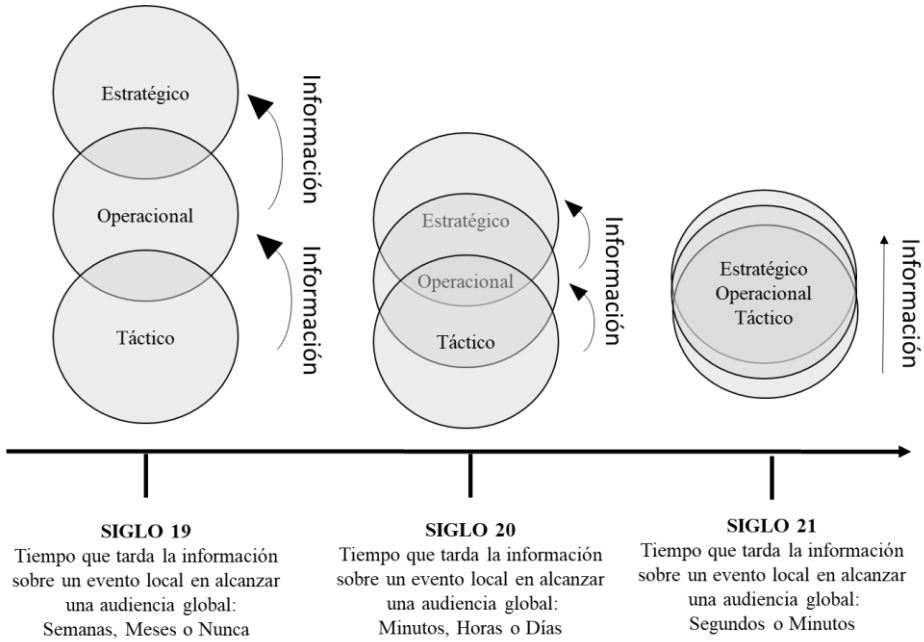
Dada la relevancia de las OI en el campo de combate multidominio, los Estados Unidos de América (EE.UU.) creó en el año 2017, la carrera Dominio de la Información, incluyendo especialistas de ciberseguridad, guerra electrónica y operaciones de información. En el mismo año, el Presidente de la Junta de Jefes de Estado Mayor de los EE.UU. aprobó incluirlas como una función conjunta. Siguiendo esta misma línea de pensamiento, el ejército de los EE.UU. considera agregarlas como una séptima

función de combate (Vertuli & Loudon, 2018, p. 135). Por su alcance y la capacidad de ser ejecutadas por cualquiera de las tres Fuerzas Armadas (FFAA) de la República Argentina las OI deberían considerarse como una función conjunta. A su vez, para que las mismas sean eficaces, tienen que ser ejecutadas bajo una misma línea de planeamiento y dirección dentro del Teatro de Operaciones.

Un aspecto sumamente importante que se debe tener en cuenta acerca de las OI dada su naturaleza instantánea, global y constante, es la capacidad que tienen de comprimir y amalgamar los niveles de la guerra. Según la Publicación Doctrinaria de la Infantería de Marina de EE.UU. (Department of the Navy, 2022, c. 1, pp. 10-13), este fenómeno es producto de la creciente interconexión global y el avance de las TIC. Los niveles de guerra se ven reducidos dado que existe una mayor cantidad y calidad de información disponible, lo que permite acortar y acelerar el proceso de toma de decisiones y reducir el tiempo de respuesta en situaciones de crisis y conflictos. La facilidad con la que la información se difunde en todo el mundo permite al público monitorear continuamente los eventos locales a escala global, consiguiendo que acciones tácticas tengan consecuencias de nivel estratégico.

Figura 1

La Información Comprime los Niveles de la Guerra



(Department of the Navy, 2022, c. 1, p. 11)

La necesidad de comprender e incorporar las OI como una nueva capacidad para las FFAA, se ve reflejada en la Directiva de Política de Defensa Nacional (DPDN) 2021,

la cual reconoce que hay nuevos factores en el ambiente operacional que se deben analizar “es necesario explorar la posibilidad de nuevos efectos militares a partir de la combinación del conocimiento tradicional de empleo con formas innovadoras basadas en tecnología, conocimiento y aprovechamiento dual” (Poder Ejecutivo Nacional, 2021, p. 21). A su vez, también determina que durante el Planeamiento Estratégico Militar, se deberá realizar: “El mejor aprovechamiento posible de los grandes espacios jurisdiccionales a través del despliegue de elementos que favorezcan una estrategia disuasiva, priorizando las acciones de guerra cibernética, información, energía dirigida y vehículos no tripulados” (Poder Ejecutivo Nacional, 2021, p. 34).

La anexión de la península de Crimea a la Federación de Rusia (FR) es un hecho histórico que permite estudiar las tácticas y estrategias utilizadas de OI, así como sus efectos en la opinión pública. Este caso permite analizar y sacar conclusiones sobre cómo las OI pueden ser utilizadas como una herramienta estratégica en los conflictos, permitiendo a los actores moldear la percepción pública, influir en las narrativas, obtener ventajas políticas y alcanzar los objetivos operacionales (OO).

A lo largo de los años, la FR se ha destacado como uno de los países que ha utilizado activamente las OI como una herramienta estratégica en su enfoque geopolítico. En los últimos años, ha mostrado un alto grado de sofisticación y persistencia en el uso de las OI con fines políticos y militares. Empleando una combinación de tácticas que incluyen desinformación, propaganda, ciberataques y manipulación de las redes sociales (RS) para influir en la opinión pública y lograr sus objetivos estratégicos.

En 2007, Estonia experimentó un conflicto con Rusia conocido como la crisis de los monumentos. La tensión se desató después de que el Gobierno estonio decidiera reubicar un monumento soviético llamado el Soldado de Bronce, que conmemoraba a los soldados soviéticos que murieron en la Segunda Guerra Mundial. La reubicación del monumento generó protestas por parte de la minoría rusa en Estonia, quienes lo veían como un símbolo de su herencia soviética y consideraban que su traslado era un acto de desprecio hacia su identidad. Las protestas se intensificaron y derivaron en disturbios y enfrentamientos violentos en Tallin, la capital de Estonia (Mc Guinness, 2017).

En respuesta a los disturbios, Rusia llevó a cabo una ofensiva de dos fases, inicialmente se realizó una serie de ciberataques contra los sitios web del partido político que lideraba el Gobierno de Estonia. Posteriormente, en una segunda fase, los ataques se intensificaron, buscando sobrecargar los servidores de computadoras de Estonia con enormes volúmenes de tráfico de mensajes falsos, causando que se colapsaran,

produciendo interrupciones en los servicios gubernamentales y financieros del país. Algunas estimaciones sugieren que un millón de computadoras fueron cooptadas, o de otra forma empleadas globalmente por esta arremetida de denegación de servicio, sobre los servidores de un país de 1,3 millones de habitantes (Vertuli & Loudon, 2018, p.213).

En 2008, se produjo un conflicto armado entre Georgia y Rusia originado en las tensiones existentes entre Georgia y las regiones separatistas de Osetia del Sur y Abjasia, que habían declarado su independencia, pero no eran reconocidas internacionalmente. El 7 de agosto de 2008, Georgia lanzó una ofensiva militar contra Osetia del Sur en un intento por recuperar el control de la región. En respuesta, Rusia intervino militarmente en apoyo a Osetia del Sur. Las Fuerzas Rusas llevaron a cabo una operación militar, desplegando tropas y bombardeando objetivos militares y civiles en Georgia. Durante este conflicto, se llevaron a cabo diversas OI que jugaron un papel crucial en la percepción pública y en la narrativa del conflicto.

> Los ataques cibernéticos a los sistemas de Georgia ya estaban en ejecución antes que Rusia invadiera en 2008. El día que comenzaron los ataques terrestres, sitios como stopgeorgia.ru publicaron listas de objetivos georgianos para atacar, así como instrucciones sobre cómo lanzar esos ataques. Mientras Moscú provocaba a Georgia con movimientos de tropas en las fronteras de las provincias separatistas de Abjasia y Osetia del Sur, los *bots*[1] ya estaban en el ataque degradando sitios web georgianos, incluyendo las páginas del presidente, el parlamento, el ministro de relaciones exteriores y agencias de noticias. Los bancos, que también eran blancos del ciberataque, apagaron sus servidores al primer indicio de ataque, para prevenir el robo de identidad o dinero. Esta fue la primera (reconocida) vez que ataques rusos, cibernéticos y militares tradicionales, fueron llevados a cabo en coordinación (Vertuli & Loudon, 2018, p. 213).
>
> El pensamiento militar ruso entiende que la información es una fuente de poder.
>
> El enfoque ruso en la información y la superioridad de la información es un elemento importante en las doctrinas y estrategias del país. La Estrategia de Seguridad Nacional 2020, establece en su análisis de futuras amenazas que la lucha global por la información se intensificará (Jaitner & Mattsson, 2015, p. 40).

[1] Programa informático que realiza tareas automatizadas específicas y, generalmente, repetitivas en una red. (Real Academia Española, 2022)

Igor Panarin, politólogo y analista ruso, ha expresado varias teorías relacionadas con las OI. Sus puntos de vista se han centrado principalmente en la geopolítica y las estrategias de influencia. En su obra, Guerra de la Información y Comunicaciones, describe los instrumentos básicos involucrados en las OI, identifica la propaganda negra, gris y blanca; la inteligencia, recopilación de información; el análisis, seguimiento de medios y análisis de situación; y la organización, coordinación y conducción de canales e influencia en los medios para formar la opinión de políticos y MCS. En términos de operaciones de influencia, Panarin identifica los siguientes métodos: el control social, la maniobra social, la manipulación de la información, la desinformación, creación de información falsa, el chantaje y la extorsión (Iasiello, 2017, p. 52).

Pensadores como Ivan Vorobyev y Valery Kiselyov consideran que, "La información se ha convertido en un arma. No es solo una adición a la potencia de fuego, ataque, maniobra, sino que transforma y une todo esto" (Jaitner & Mattsson, 2015, p.41).

A finales de enero de 2013, el General Valery Gerasimov, Jefe del Estado Mayor General ruso, pronunció un discurso ante la Academia de Ciencias Militares. El texto fue publicado por Voienno-Promyshlenny Kurier bajo el título, "El valor de la ciencia está en la previsión" (Gerasimov, 2013). El General sugiere que, las reglas de guerra han cambiado, el valor de los medios no militares para lograr los fines políticos y estratégicos no solo se han incrementado, sino que en algunos casos excede la efectividad de las armas. Señala que, las nuevas tecnologías han reducido la brecha entre las fuerzas tradicionales y su comando y control. También menciona que, los grandes enfrentamientos entre fuerzas armadas en el nivel estratégico y operacional son cosas del pasado. En el futuro, las acciones militares serán acciones sin contacto, ejecutadas mediante medios cibernéticos y OI (Gerasimov, 2013).

Complementariamente, Gerasimov propone medidas militares y no militares para llevar adelante un conflicto. Identifica como medidas no militares: la presión política y diplomática; las sanciones económicas; los bloqueos económicos; el cese de relaciones diplomáticas; la formación de la oposición política. También, sugiere otras formas de resolver el conflicto, por ejemplo, incitar a un cambio de liderazgo político en el país opositor a Rusia o buscar el apoyo de los MCS. Propone realizar operaciones convencionales coordinadas con operaciones no convencionales e irregulares; ejecutar medidas de disuasión estratégica militar con fuerzas convencionales; despliegues estratégicos disuasorios; operaciones militares puntuales; uso de misiles hipersónicos no nucleares; utilizar ciberataques y ciberdefensa; realizar operaciones de estabilidad y

consolidación bajo el paraguas de operaciones de paz; recurrir a sus fuerzas nucleares estratégicas como amenaza (Gerasimov, 2013/2016).

Makotczenko (2019, pp. 21-22) concluye que, los conceptos expresados por Gerasimov son una nueva forma de instrumentar la estrategia militar, la cual utiliza todos los métodos que posee el Estado para el logro del objetivo impuesto por la estrategia nacional. Sostiene que en los conflictos actuales se deben tener en cuenta metodologías que anteriormente no se consideraban, como por ejemplo los medios de presión económica, política, diplomática, informativa e informática.

Otros autores ya han abordado el conflicto de Crimea en 2014, Belletti (2021) en su investigación describe las causas del enfrentamiento entre la FR y Ucrania, detalla la importancia que reviste la península de Crimea para el Gobierno ruso. Posteriormente, detalla las operaciones cibernéticas ejecutadas y centra su investigación en determinar cómo su utilización contribuyó al logro de los objetivos establecidos por el nivel operacional.

Por otro lado, Policante (2019) desarrolla el conflicto de Crimea analizando ¿Cuál fue el rol de las fuerzas armadas en las operaciones interagenciales en el marco de una guerra híbrida?

Si bien todavía no se ha escrito doctrina específica sobre OI diferentes autores nacionales han definido su concepto.

> […] conjunto de operaciones y actividades que consiste en el uso ofensivo y defensivo de la información y de los sistemas de información destinados a manipular, explotar, destruir y degradar la información y sistemas de información del enemigo, procurando al mismo tiempo la protección de los sistemas propios a fin de obtener la superioridad en el ámbito de la información (Ferrari, Vigón, Gaggero, 2001, p. 66).

Para Stel (2005), el objetivo de las OI es “dañar, destruir o modificar la información contenida en las redes y sistemas para generar un cambio en lo que la población piensa o conoce” (p. 55).

Los autores de Vergara & Trama (2016) definen las OI como:

> […] aquellas que implican el uso y manejo de la tecnología de la información y la comunicación para acceder, modificar, interrumpir, alterar o destruir la información del oponente en procura de obtener una ventaja competitiva, así como asegurar la integridad de la información propia (p. 256).

Seis años después del conflicto de Georgia, Rusia aplicó las lecciones aprendidas referidas a las OI ejecutadas en esa guerra, durante el desarrollo de las acciones en la península de Crimea.

La guerra de Crimea en 2014 fue un conflicto entre Ucrania y Rusia que se desencadenó después de que las protestas populares en Ucrania derrocaran al presidente Viktor Yanukovich, quien era un aliado cercano de Rusia. El pueblo ucraniano estaba dividido entre aquellos que querían una mayor integración con Rusia y los que apoyaban una mayor alianza con la Unión Europea (UE). Tras el derrocamiento del presidente, el parlamento de Crimea eligió a un primer ministro prorruso y votó mediante un referéndum a favor de separarse de Ucrania con aproximadamente un 95% de votos a favor. Rusia oficializó la anexión firmando un proyecto de ley en el que Crimea se incorporaba a la FR. La noticia de la anexión recibió condena internacional considerando que se estaba violando la soberanía de Ucrania y el derecho internacional.

"Cuando la crisis de Ucrania llegó a su primer pico con la anexión de la península de Crimea, quedó claro que Rusia estaba llevando a cabo intensas operaciones de información y, más aún, que estaba teniendo éxito con estas" (Jaitner & Mattsson, 2015, p. 40).

Rusia utilizó una amplia variedad de OI durante el conflicto, estas operaciones estaban diseñadas para influir en la opinión pública tanto en Rusia como en el extranjero y para justificar su intervención en el conflicto. A diferencia de los ataques digitales y el cruce fronterizo militar en Georgia, mediante la guerra de la información ejecutada contra Crimea, las Fuerzas Rusas cerraron la infraestructura de telecomunicaciones, desactivaron los principales sitios web ucranianos y bloquearon los teléfonos celulares de los principales funcionarios ucranianos antes de su ingreso a la península el 2 de marzo de 2014 (Iasiello, 2017, p. 54).

> […] La estrategia militar rusa tiene como objetivo desestabilizar rápidamente países estables mediante acciones no militares. Los métodos rusos se centran en localizar y explotar las debilidades y divisiones internas de un país para socavar su sociedad. Estas acciones pueden incluir el empleo del potencial de protesta de la población, las fuerzas de operaciones especiales y medidas militares y de guerra de información encubiertas (Cockrell, 2018, p. 5).

Finalmente, es necesario mencionar que, en el ámbito castrense, no hay doctrina referida a las OI, solo han sido definidas en el Glosario de términos de empleo militar

para la acción militar conjunta. Para la realización de este trabajo se utilizará la definición publicada en el mencionado reglamento:

> Acciones que implican el uso y manejo de la tecnología de la información y las comunicaciones, dentro de las dimensiones físicas, de información y cognitivas del ambiente de la información, en concierto con otras líneas de operaciones, para acceder, modificar, interrumpir, alterar o destruir la toma de decisiones del adversario, protegiendo, al mismo tiempo, las propias (Estado Mayor Conjunto de las Fuerzas Armadas, 2019, p. 136).

Según Motta (2023, p. 23), las fuerzas militares requieren de un periodo de tiempo para adiestrarse correctamente en nuevas capacidades. Los escenarios actuales que están altamente conectados y globalizados exigen que las soluciones no sean únicamente mediante el empeño tradicional de la fuerza militar, por lo cual, es importante conocer cuáles son las nuevas formas de realizar la guerra y capacitarse para poder desarrollarlas.

En función de lo descrito anteriormente, donde se ve reflejado que en los conflictos actuales se utilizan métodos militares y no militares utilizando herramientas no convencionales para llevar a cabo las operaciones, es necesario analizar y comprender cómo ejecutar OI para poder alcanzar los objetivos establecidos y no quedar obsoletos frente a un enemigo que constantemente se capacita en las nuevas formas de realizar la guerra. Rusia es uno de los principales países que ejecuta OI por tal motivo es que surge el interrogante que origina el desarrollo del presente trabajo final integrador ¿De qué manera las operaciones de información ejecutadas por las fuerzas de la Federación de Rusia, durante en el conflicto con Crimea en 2014, contribuyeron al cumplimiento de los objetivos operacionales?

A través del presente trabajo, solo se llevará a cabo un análisis de las OI implementadas por la FR en el contexto de la anexión de la península de Crimea en el año 2014. Inicialmente, se analizará la metodología empleada por Rusia en la ejecución de OI, sus objetivos al ejecutarlas, las principales características, los métodos que utiliza y la estructura organizativa. Posteriormente, se procederá a identificar las causas que condujeron a este enfrentamiento, la relevancia que la península de Crimea tiene para el Gobierno ruso. Se mencionarán los OO que se establecieron, se analizará la planificación de la campaña informativa, y se detallarán las OI que se llevaron a cabo como parte de esta estrategia.

Por último, es necesario aclarar que el desarrollo de esta investigación se centrará exclusivamente en las OI llevadas a cabo durante el conflicto entre la FR y Ucrania. No

serán objeto de estudio las operaciones cibernéticas, ni su contexto operacional híbrido, ya que estas áreas de investigación han sido abordadas anteriormente.

A través de este caso histórico se pretende proporcionar un análisis concreto y específico de las OI efectuadas durante el conflicto mencionado. Para obtener conclusiones sobre la ejecución de estas operaciones y su impacto en el cumplimiento de objetivos del nivel operacional. A su vez, se pretende demostrar cómo ha ocurrido un cambio radical en el caracter de la guerra, destacando que es necesario adaptarse y no correr el riesgo de no estar preparados para el próximo conflicto.

En la República Argentina no existe doctrina sobre OI, por lo cual es necesario comenzar a incorporar las lecciones aprendidas que brindan los conflictos armados más recientes y establecer las bases necesarias para poder desarrollarlas en el futuro.

Para dar respuesta al problema planteado, se ha determinado un objetivo general que consiste en describir las operaciones de información ejecutadas por las fuerzas de la FR, durante el conflicto en Crimea en 2014. En concordancia con el objetivo general, el trabajo se desarrollará en dos capítulos. En el primer capítulo, se analizará la metodología empleada por Rusia en la ejecución de OI, sus objetivos al ejecutarlas, las principales características, los métodos que utiliza y la estructura organizativa que posee la FR. Posteriormente, en el segundo capítulo, se analizará la campaña de información que realizaron las fuerzas de la FR, durante el conflicto en Crimea en 2014.

Finalmente, y como parte del proceso metodológico, la investigación se desarrollará sobre la base del método deductivo, buscando cumplimentar el objetivo general y los dos objetivos específicos. Arribar a los objetivos particulares permitirá obtener conclusiones parciales que contribuirán a dar respuesta al objetivo general.

El diseño será de tipo descriptivo, a fin de responder a los objetivos planteados en el presente plan de trabajo. Se realizará un estudio analítico-descriptivo de los hechos históricos en función de los conceptos relacionados y las OI ejecutadas por las fuerzas de la FR que permitan dar una respuesta al problema planteado.

Para realizar la investigación se utilizarán documentos legales vigentes, libros, artículos académicos, informes, trabajos finales y reglamentos militares, todos provenientes de fuentes abiertas.

Capítulo I

Operaciones de Información Rusas

1.1 Teoría de las Operaciones de Información Rusas

Rusia históricamente ha realizado OI influenciadas por una combinación de factores históricos, políticos y tecnológicos. Esta estrategia se ha desarrollado y evolucionado a lo largo del tiempo, y su historia se entrelaza con la evolución política y militar de Rusia y la Unión de Repúblicas Socialistas Soviéticas (URSS).

Iasiello (2017) describe que, durante la Guerra Fría, la URSS compitió con Occidente, especialmente con los EE.UU., en una rivalidad geopolítica. En este contexto, la desinformación y la propaganda se convirtieron en herramientas esenciales de influencia política y manipulación de la percepción pública. La URSS desarrolló una sofisticada maquinaria de propaganda que se extendió por su propio territorio y a nivel internacional. Esto incluyó la creación de MCS controlados por el Estado, como *Pravda*, y la difusión de narrativas favorables al régimen comunista en el extranjero. La propaganda soviética se centró en desacreditar a Occidente y promover la imagen de la URSS como un modelo de éxito socialista. Además de la propaganda, la URSS llevó a cabo operaciones de desinformación diseñadas para sembrar confusión y desconfianza en Occidente. Esto incluyó la creación y difusión de noticias falsas y teorías de conspiración destinadas a debilitar la cohesión de los países Occidentales. El Comité para la Seguridad del Estado (*Komitet Gosudarstvennoy Bezopasnosti* - KGB) desempeñó un papel fundamental en la realización de OI durante la Guerra Fría. La KGB estaba involucrada en la infiltración de grupos de influencia en el extranjero, la manipulación de MCS y la promoción de narrativas favorables a la URSS (p. 56).

Por último, la llegada de Internet y las RS le ha brindado a Rusia la oportunidad de llevar a cabo OI de una manera más sofisticada y global. Las plataformas digitales permiten llegar a audiencias internacionales de forma directa y rápida, permitiendo difundir información en tiempo real.

1.2 Renacimiento de las Operaciones de Información

Según el historiador Richard Pipes (1995, p. 305), el líder comunista ruso, Vladimir Lenin, concedió a la propaganda la más alta prioridad, atribuyéndole la capacidad de contribuir a que su régimen sobreviviera a los diferentes obstáculos que se le presentaban. Para él, su principal objetivo era lograr el control total sobre todas las fuentes de información.

Durante esta época, una de las principales técnicas utilizadas por la URSS fue el ocultamiento, conocida como *maskirovka*, ya que se consideraba que esta acción otorgaba cierto grado de control sobre un adversario al inducirlo a tomar una decisión errónea, por su propia voluntad. Mediante esta teoría, denominada control reflexivo, se aprecia cómo se buscaba influir en la percepción del oponente sobre la situación, sus objetivos o su doctrina, y al mismo tiempo ocultarle el hecho de que se lo estaba influenciando (Wilde & Sherman, 2023).

Según Darczewska (2014, p. 9), el Instituto Militar de Idiomas Extranjeros fue el primer organismo educativo que dictó la materia *spetspropaganda* (propaganda especial), en el año 1942. Posteriormente, fue eliminada del plan de estudios en la década de los 90 para finalmente reintroducirse a principios del año 2000. Luego de una serie de reformas, el instituto ha pasado a ser el Departamento de Información Militar e Idiomas Extranjeros de la Universidad Militar del Ministerio de Defensa de la FR. Las diferentes modificaciones en los planes de estudios del instituto son un claro ejemplo del cambio de enfoque que ha realizado el Gobierno ruso sobre la importancia de las OI.

En la actualidad, la FR emplea la doctrina Gerasimov. Esta doctrina refleja una comprensión de las guerras y los conflictos en la era moderna que se aleja de la concepción tradicional de la guerra. Gerasimov reconoce que la naturaleza de la guerra ha evolucionado, ya no se trata simplemente de enfrentamientos militares convencionales en el campo de batalla, sino que involucra una mezcla de medidas militares y no militares que se ejecutan de manera coordinada. Uno de los elementos más destacados de esta doctrina es la idea de que las medidas no militares deben prevalecer sobre el poder militar. En otras palabras, Rusia prioriza el uso de herramientas como la desinformación, la manipulación de la opinión pública, la infiltración política y la influencia económica para alcanzar sus objetivos antes de recurrir a la fuerza militar convencional. Este enfoque sugiere que el poder militar debe utilizarse solo cuando las medidas no militares no logran alcanzar los objetivos deseados (Bilyana & Cheravith, 2020, p. 132).

1.3 Objetivos de las Operaciones de Información Rusas

A diferencia de otros países, Rusia no solo ejecuta OI para apoyar sus operaciones militares, buscando ablandar al enemigo o preparando el campo de combate para las futuras acciones, sino también busca concretar otra clase de objetivos. Sus intervenciones armadas, como en Ucrania, están subordinadas a un objetivo estratégico, normalmente orientado a desafiar los intereses del mundo occidental y evitar que los

concreten. Es así como se observa que en ocasiones las OI rusas se aplican para la obtención de objetivos políticos sin la necesidad que haya una operación militar en curso, no hay que olvidar que las OI son un medio barato y efectivo para concretarlos sin derramar sangre y muchas veces amparadas en el anonimato (Vertuli & Loudon, 2018, p. 65).

Como afirmó Cheravitch (2021, p. 4-5) en su artículo, casi todos los autores, mantienen una definición separada para la guerra de información y la confrontación informativa, y agregó que la guerra de información debería excluirse de documentos oficiales, ya que el término *warfare (guerra*) connota conflicto armado, que está ausente en el tipo de competencia digital en tiempos de paz a la que suelen hacer referencia los autores militares rusos. Expertos occidentales señalan que, no existe una distinción real entre los conceptos guerra cibernética y guerra de la información, que combinan de manera indivisible los aspectos físicos y psicológicos de la competencia interestatal moderna a través de la tecnología de la información.

El diccionario enciclopédico militar del Ministerio de Defensa de Rusia define la confrontación informativa como una forma de conflicto entre bandos opuestos que buscan derrotar al enemigo a través de efectos informativos en la esfera de la información, al tiempo que resisten o reducen tales efectos por parte de uno mismo (Grisé, 2022, p. 7).

Según la autora, los militares rusos identificaron dos subtipos de confrontación de la información: la informativa-psicológica y la informativa-técnica.

La primera incluye esfuerzos para influir en la población y las fuerzas militares del enemigo, engañándolo, socavando su voluntad de resistir, produciendo pánico en sus filas y traición. Puede ser ofensiva o defensiva y está dirigida a los pensamientos del enemigo y a la defensa de los propios pensamientos. El personal militar no solo participa activamente en la confrontación de información, sino que ellos mismos son un objeto de continua influencia informativa-psicológica. A su vez, permite controlar la mente del enemigo, ya sea directa o indirectamente, mediante la introducción de información específica, sobre la base de la cual, el adversario, toma una decisión (p. 11-12).

El subtipo informativo-técnico implica la manipulación física de RS y herramientas de información, la destrucción de información, redes radio electrónicas, e informáticas, y obtener acceso no autorizado a los recursos de información del enemigo. Buscando influir en las redes de comunicación y las redes de información utilizadas por las organizaciones gubernamentales en el desempeño de sus funciones de gestión, la

infraestructura de información militar, las estructuras de información y gestión de las empresas industriales y de transporte, y los medios de comunicación (p. 12).

La doctrina rusa de OI se centra principalmente en una estrategia de influencia llamada control reflexivo. Snegovayana (2015, p. 21) señala que, el control reflexivo es una forma de transmitir a un compañero u oponente información especialmente preparada para inclinarlo a tomar voluntariamente la decisión predeterminada deseada por el iniciador de la acción, en otras palabras, es una forma de influir al oponente para que, sin saberlo, tome malas decisiones.

Según Snegovaya (2015, pp. 13-14), los objetivos perseguidos por las Fuerzas Rusas en las OI son cuatro: negar (dismiss), distraer (distract), falsear (distort) y consternar (dismay).

La negación permite desestimar información o acusaciones desfavorables; las Fuerzas Rusas a menudo utilizan tácticas de negación y rechazo para contrarrestar las críticas o las acusaciones de comportamiento indebido. Para ello pueden negar su participación en acciones como ciberataques, desestabilización política o violaciones de derechos humanos. Esta negación no solo generará dudas en la opinión pública, sino que también perjudicará la credibilidad de quienes presentan las acusaciones.

La distracción es una táctica recurrente en las OI rusas, consiste en desviar la atención de temas o situaciones desfavorables para el Gobierno ruso y enfocarla en otros asuntos o controversias. Por ejemplo, cuando se enfrentan a críticas o sanciones internacionales, las Fuerzas Rusas pueden distorsionar un evento para acaparar la atención mediática y distraer a la comunidad internacional de problemas más graves.

La distorsión de la información es otro objetivo clave de las OI rusas, implica la manipulación de hechos, la promoción de narrativas falsas o la creación de teorías de conspiración con el fin de sembrar confusión sobre la verdad objetiva. La distorsión puede utilizarse para cambiar la percepción de eventos o para impulsar agendas políticas específicas. Esta táctica se ha vuelto más efectiva en la era de las RS y la información en línea, dado su alcance masivo y sin fronteras.

La consternación busca socavar la confianza en las instituciones y la estabilidad de los países Occidentales y de sus aliados. Las OI rusas a menudo buscan crear divisiones internas, fomentar la polarización política y exacerbar tensiones existentes en países extranjeros. El objetivo es debilitar la cohesión y la resistencia de los países Occidentales, lo que puede ser beneficioso para los intereses geopolíticos de Rusia.

A través de las OI también se buscará realizar la recopilación y manipulación de datos, se implementarán medidas políticas activas y se desarrollará la guerra económica. Complementariamente, se intentará dañar la reputación de los adversarios a través de afirmaciones verdaderas o falsas referidas a abusos sexuales, discriminación racial, corrupción, que causen una reacción popular. Económicamente, se manipulará la infraestructura de transporte para generar desabastecimiento de productos, también se activarán dispositivos de células dormidas para recolectar información interna activa o pasivamente. Estas líneas de operaciones se realizarán evitando que sean detectadas, para no quedar expuestos, ya que en caso de ser descubiertos, la operación en curso perderá credibilidad y afectará las futuras. Esto permitirá, que las Fuerzas Rusas dedicadas a las OI se movilicen bajo una red de camuflajes sostenida en el ocultamiento de información (Vertuli & Loudon, 2018, pp. 54-55).

"Las consecuencias en la audiencia objetivo son claras: desmoralización, desconfianza en los ciudadanos hacia las autoridades y el sistema y hasta en la posibilidad de discernir qué sucede y por qué" (Iglesisas Sanchez, 2021, p. 58).

1.4 Características de las Operaciones de Información Rusas

Es necesario aclarar que entienden las Fuerzas Rusas por OI, estas operaciones son consideradas como una herramienta que permite lograr algún tipo de objetivo táctico limitado o ventaja durante el conflicto. Mediante su ejecución buscan degradar la capacidad del enemigo para controlar el espacio informacional, negarle la capacidad técnica para tomar represalias a través de medios del ciberespacio y defender la narrativa de nacionalismo ruso, para glorificar su papel en el escenario mundial. Las OI rusas incluyen una gran cantidad de innovaciones tácticas, desde operaciones psicológicas hasta comunicaciones estratégicas dirigidas a controlar la narrativa y modificar la percepción de la audiencia, incluyendo el despliegue de sofisticados trolls[2] y bots descentralizados en RS y páginas web (Vertuli & Loudon, 2018. pp 31-32).

El concepto holístico que tiene Rusia sobre las OI, permite que sean usadas tanto con fines militares como políticos. A su vez, favorece el trabajo mancomunado con las operaciones cibernéticas, guerra electrónica, operaciones psicológicas, etc. Por otro lado, a diferencia de las potencias de Occidente, que su doctrina establece que este tipo

[2] En foros de internet y redes sociales, publicar mensajes provocativos, ofensivos o fuera de lugar con el fin de boicotear algo o a alguien, o entorpecer la conversación. (Real Academia Española, 2022)

de acciones solo se realizan durante tiempo de guerra, las Fuerzas Rusas las ejecutan para obtener una ventaja del enemigo, ya sea en tiempos de paz o de guerra.

1.4.1 Naturaleza Interdisciplinaria de las Operaciones de Información

El enfoque ruso sobre las OI es mucho más amplio que el de los países Occidentales, su planeamiento se realiza de forma integral y holística. La mente de los individuos y los sistemas de información siempre han formado parte de las estrategias de seguridad rusas. En cambio, para los países Occidentales el ámbito cognitivo no siempre es considerado como parte del ambiente informacional. Todas las capacidades relacionadas con la información que en otros países tienen diferentes dependencias en Rusia están unificadas y dependen del Estado Mayor General Ruso.

En el año 2000 fue publicada la Doctrina de Seguridad de la Información de la Federación Rusa (Putin, 2000), este documento generó un rápido aumento de interés sobre todos los temas relacionados con la información y su seguridad. Incluyendo la formación teórica sobre OI en los planes de estudio de los establecimientos de educación superior y en proyectos realizados por institutos de investigación y ciencia. Como resultado de este incremento de interés, los cursos de formación de diplomáticos dictados en el Instituto Estatal de Relaciones Internacionales de Moscú y la Academia Diplomática del Ministerio de Relaciones Exteriores de la FR, así como los planes de estudios en los departamentos de sociología, filosofía y ciencias políticas de otras universidades ahora incluyen temas tales como: análisis de situación, tecnología de comunicación en red y guerras de información y redes.

Este auge por el estudio e investigación sobre las OI ha generado que se las considere como una ciencia interdisciplinaria. Esto se debe a que abarcan una gama muy amplia de áreas de interés (políticas, económicas, sociales, militares, de inteligencia, contrainteligencia, diplomáticas, propagandísticas, psicológicas, informáticas, tecnologías de la comunicación, educativas, etc.). Durante la última década, la FR ha creado varios centros de investigación destinados a estudiar diferentes áreas dentro de las OI (Darczewska, 2014, p. 10).

1.4.2 Técnicas Comunicacionales

Según Vertuli y Loudon (2018, p. 64), las OI rusas se sustentan en tres técnicas comunicacionales que se interrelacionan para obtener los resultados esperados.

La primera técnica que utiliza es presentar las noticias ordinarias, buscando resaltar aquellos aspectos que benefician su narrativa. Lo hace a través de medios controlados

por el Estado como el canal de televisión RT ex *Rusia Today*, la emisora de radio *Sputnik*, la red social *Vkontakte*, así como a través de otros medios de difusión que dan servicio a la población ruso parlante de los ex Estados Soviéticos. Este nuevo enfoque de las noticias generalmente sugiere a Rusia como una mejor alternativa contraria a las ambiciosas y agresivas naciones Occidentales.

En segundo lugar, utiliza la desinformación para crear ambigüedad para confundir a las personas, tanto en el país como en el extranjero, sobre sus operaciones, ya sea en Ucrania, Siria, África o en cualquier parte del mundo donde se encuentre operando, ya que su principal objetivo es contribuir a la niebla de guerra.

La última técnica comunicacional consiste en mentir cuando se le da información verdadera, afirmando que es falsa. Esta última estrategia tiene varios objetivos: degradar la confianza en las instituciones de todo el mundo; presionar a poblaciones en conflicto para aceptar el statu quo del conflicto y no presionar por una pronta resolución; y finalmente, evitar que países que integran su esfera de interés ingresen a alianzas Occidentales como la Organización del Tratado del Atlántico Norte (OTAN), manteniendo a los mismos en perpetuo conflicto.

1.5 Principales Métodos para Ejecutar Operaciones de Información

Las Fuerzas Rusas utilizan cinco métodos para ejecutar las OI: la manipulación de información (noticias falsas), el espionaje (inteligencia), la interferencia política, el engaño militar (negación creíble) y la manipulación de las RS. Este último es el único elemento que es realmente nuevo e innovador, ya que permite influenciar una mayor cantidad de personas sin distancias físicas (Vertuli & Loudon, 2018, pp. 68-71).

1.5.1 Manipulación de Información

Las Fuerzas Rusas han dominado el uso de noticias falsas y la desinformación para confundir o persuadir al público blanco seleccionado, tanto en Rusia como en Occidente. El objetivo es erosionar el apoyo público y la confianza en las instituciones democráticas Occidentales, mediante la generación de discordia pública y política para crear confusión con el fin de influir a los tomadores de decisiones en los más altos niveles e intensificar la competencia en seguridad en áreas de importancia estratégica tanto para Occidente como para Rusia. Esta técnica es especialmente utilizada en Europa del Este y el sur del Cáucaso a lo largo de la línea divisoria entre la OTAN y los países que alguna vez orbitaron dentro de la esfera de influencia de la URSS, principalmente los Países Bálticos, Georgia y Ucrania. Intensificar la competencia le permite condicionar a los adversarios de Rusia, provocarlos e influir en sus públicos para

desaprobar la toma de cualquier clase de medidas de represalia. Otro subproducto de este uso de las OI es apoyar directa e indirectamente a grupos antisistemas, partidos y políticos en Occidente, como una manera de proporcionarles una apariencia de legitimidad y dificultar los procesos democráticos.

1.5.2 Espionaje

Mediante el espionaje, los agentes del Kremlin han logrado robar materiales comprometedores e información sobre el enemigo. "En el contexto de la guerra, el actor que es más capaz de predecir e imitar el razonamiento y las acciones de su oponente, tiene la mayor probabilidad de éxito" (Snegovaya, 2015, p. 10).

Durante la Guerra Fría, los oficiales de inteligencia de la KGB fueron los encargados de realizar esta técnica. Actualmente, la realizan sus tropas de información, entre sus objetivos se encuentra perturbar las telecomunicaciones del enemigo o sistemas de almacenamiento de datos; interferir las elecciones democráticas en Occidente, ya sea mediante la liberación de información sensible, provocación por Internet, publicación de noticias falsas u otras tácticas que consideren que afectarán los sistemas democráticos de Occidente.

1.5.3 Interferencia Política

La interferencia política en los comicios electorales extranjeros no es un fenómeno nuevo en la historia de las relaciones internacionales, y no solo la ejecutan las Fuerzas Rusas, sino que ha experimentado una evolución significativa en las últimas décadas, especialmente con la aparición de tecnologías de la información y comunicación avanzadas. Este método ya no se limita a la acción de estados extranjeros en secreto, sino que ahora involucra el empleo de hackers[3] respaldados por estados nación y la influencia masiva que se puede ejercer a través de las RS.

Uno de los cambios más notables en la interferencia política implementado por los rusos es el uso de hackers para llevar a cabo ciberataques y operaciones de desinformación. Estos hackers pueden infiltrarse en sistemas informáticos de partidos políticos, gobiernos y organizaciones relacionadas con las elecciones para robar información confidencial, manipular datos o interrumpir procesos electorales. Este procedimiento permite interferir en la integridad de las elecciones de manera encubierta.

[3] Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. (Real Academia Española, 2022)

El Kremlin ya no se limita a la manipulación puntual de un evento electoral, sus estrategias son a largo plazo para debilitar la estabilidad política de un país extranjero y debilitar su posición en el escenario internacional.

1.5.4 Engaño Militar

El cuarto método que utilizan las Fuerzas Rusas para llevar adelante sus OI es el engaño militar, *maskiroyka*, para generar confusión en el enemigo. Un claro ejemplo fue cuando el Gobierno ruso negó la presencia de fuerzas militares en Ucrania. Su objetivo es distraer y ocultar la existencia de una campaña militar para evitar una respuesta más fuerte de Occidente y debilitar una posible reacción violenta en propio territorio si los hechos reales de las operaciones, incluyendo las bajas, toman estado público. El Gobierno ruso, en vez de aceptar la utilización de este método, atribuye estos ataques a patriotas rusos operando por su propia cuenta. Este tipo de campaña de desinformación es muy difícil que sea producto del trabajo de una red descentralizada de activistas improvisados, para llevarla a cabo es necesario un esfuerzo de nivel nacional fuertemente estructurado, para facilitar el logro de los objetivos estratégicos.

1.5.5 Manipulación de las Redes Sociales

Las RS y plataformas en línea brindan la capacidad de difundir desinformación y propaganda de manera masiva y a una audiencia global. Las tropas de OI rusas pueden ejercer una gran influencia en la percepción del público blanco a través de estas plataformas y agregar mayor velocidad y sofisticación a sus campañas, mediante el uso de cuentas falsas, bots, sitios web apócrifos, etc., para propagar información falsa o sesgada que influya en la opinión pública.

1.6 Organización

El Gobierno ruso ha desarrollado una estructura compleja y multifacética para llevar a cabo OI en el extranjero. Estas operaciones son parte integral de su estrategia para influir en la percepción pública, desestabilizar a países extranjeros y promover sus intereses geopolíticos. Según Wilde y Sherman (2023) su estructura es la siguiente:

- La Agencia de Inteligencia Militar Rusa, es el servicio de inteligencia militar de Rusia y juega un papel fundamental en las OI. El 72º Centro de Servicios Especiales es una unidad especializada dedicada a operaciones psicológicas, desinformación e influencia en el extranjero. Estas actividades pueden incluir la promoción de teorías de conspiración, la difusión de noticias falsas y la manipulación de la opinión pública.

- El Servicio de Inteligencia Exterior de Rusia, ex KGV, se enfoca en la inteligencia exterior. Posee una dirección dedicada a emplear organizaciones de fachada falsa para amplificar y propagar narrativas específicas en el extranjero. Implica la creación de cuentas y sitios web falsos, así como la difusión de información sesgada con el objetivo de influir en la opinión pública y en la política de otros países.
- El Servicio Federal de Seguridad, además de sus competencias internas de vigilancia y censura, realiza operaciones de manipulación de información digital en el extranjero. Estas actividades las lleva a cabo a través del Centro para la Seguridad de la Información, que se centra en actividades cibernéticas para influir en la percepción pública y desestabilizar a otros países.
- Por último, las Tropas de OI (Voyska informatsionnykh operatsiy; VIO), pueden llevar a cabo una variedad de operaciones, incluida la desinformación, la guerra cibernética y la influencia en el espacio informativo. Su papel es complementar las actividades de las agencias de inteligencia y fortalecer la capacidad de Rusia para llevar a cabo OI.

En conjunto, esta estructura altamente organizada y diversificada permite que Rusia lleve a cabo una amplia gama de OI en el extranjero. Estas operaciones son parte integral de su estrategia de influencia y tienen como objetivo desestabilizar a sus adversarios, sembrar la discordia y promover sus intereses geopolíticos.

1.7 Consideraciones Finales del Capítulo

A lo largo de este capítulo, se ha descrito en detalle la estrategia y las tácticas que la FR emplea en sus OI para alcanzar diversos objetivos. Estas operaciones forman parte de una estrategia más amplia de influencia política y manipulación de la percepción pública. Son consideradas como una herramienta estratégica clave en la política exterior de Rusia. A través de una amplia gama de técnicas respaldadas por una estructura organizativa compleja, Rusia busca socavar los intereses Occidentales y promover su propia agenda geopolítica en el escenario internacional.

Las OI se han convertido en un arma muy efectiva, operando en un espacio indefinido donde las fronteras son difusas y hasta llegan a desaparecer y los actores detrás de ellas son difíciles de identificar, logrando resultados impensados hasta hace unos pocos años. Estas operaciones plantean desafíos significativos para los países afectados y han generado preocupación a nivel global.

Capítulo II

Operaciones de Información Rusas Durante el Conflicto de Crimea

2.1 Anexión de la Península de Crimea a la Federación Rusa

Desde el fin de la Guerra Fría, Rusia fue perdiendo influencia económica, política y militar en varios territorios de Europa Oriental. Mediante la toma de la península de Crimea en 2014 intentó corregir la situación. La invasión fue un evento complejo y hubo varias causas que contribuyeron a esta acción que se desencadenaron en medio de una serie de eventos políticos y tensiones históricas. La principal causa fue el derrocamiento del presidente ucraniano, Viktor Yanukovich, el 22 de febrero de 2014, luego de una serie de protestas populares contra él en Kiev, conocidas como la Revolución Ucraniana de 2014 o Euromaidán. Las manifestaciones se originaron debido a la decisión del presidente de no firmar un acuerdo de asociación con la UE, y continuar con una política de acercamiento a la FR. El pueblo ucraniano estaba dividido entre quienes querían una mayor integración con Rusia y los que apoyaban una alianza con la UE.

Hassan (2019) indica que, en Crimea, aproximadamente el 60% de la población es de origen ruso, y no estaba de acuerdo con las protestas en Kiev. Luego del cambio de Gobierno, la población solicitó ayuda a Moscú. El presidente ruso respondió con un envío de tropas especiales sin identificar, que tomaron el control de las ciudades más importantes de Crimea, así como del puerto local. Luego, Putin obtuvo el permiso del parlamento para intervenir militarmente en la península. En medio del caos político, Rusia ejecutó una operación encubierta utilizando sus fuerzas de infantería naval y sus fuerzas especiales, simulando sus movimientos de tropas, con un ejercicio militar para posteriormente tomar el control de las ciudades más importantes y el control del puerto local, también desplegó una fuerza de distracción en la frontera con Ucrania. En ese momento, las autoridades rusas declararon que el despliegue de tropas tenía el objetivo de garantizar la integridad de los rusos parlantes que habitaban en Crimea y las bases militares rusas hasta que se normalizara la situación sociopolítica. Esta operación fue exitosa porque inicialmente se preparó el campo de combate mediante diferentes OI y posteriormente las tropas convencionales consolidaron los objetivos mediante acciones tácticas.

El empleo de fuerza militar en Crimea, los hombrecillos verdes, militares rusos sin identificaciones, fue negado sistemáticamente por el Kremlin hasta que las condiciones para obtener el éxito de la operación estaban ya firmemente establecidas. A pesar de que

la operación para ocupar la península se inició el 27 de febrero, las autoridades rusas negaron su participación directa mediante diferentes OI hasta el 17 de abril de 2015 (Snegovaya, 2015, p. 17).

El 24 de febrero, el ayuntamiento de Sebastopol nombró como alcalde un ciudadano ruso, posteriormente varias unidades de infantería naval llegaron a la plaza de la ciudad en vehículos blindados en violación de las normas que rigen los arreglos de base en Crimea. Esta fue la primera señal tangible de que Rusia había decidido intervenir militarmente la península para cambiar el orden político (Kofman, y otros, 2017, p. 7).

El 16 de marzo de 2014, los rusos de Crimea convocaron a un referéndum, obteniendo como resultado que el 95% aceptaba la adhesión de Crimea a Rusia. Moscú defendió la legalidad de la votación, mientras que el Gobierno de Kiev la condenó.

La península de Crimea posee una trascendencia estratégica para Rusia debido a su ubicación geográfica. En su territorio alberga la base naval de la flota del mar Negro en Sebastopol, que es vital para la proyección de poder naval ruso en el mar Negro, el acceso al Mediterráneo y el control de las rutas comerciales. A su vez, Crimea posee una gran cantidad de recursos naturales, como reservas de gas y petróleo.

A su vez, la posible incorporación de Ucrania a la UE y la OTAN fue otro de los factores que causaron preocupación en Rusia. Por lo cual, la anexión de Crimea se percibió como un intento de evitar que Ucrania se alejara de la esfera de influencia rusa y se acercara a Occidente.

Luego de la invasión de la península, se produjo un conflicto armado en el este de Ucrania, el 06 de abril de ese año, en las regiones de Donetsk y Lugansk, donde grupos separatistas respaldados por Rusia se enfrentaron a las fuerzas ucranianas. Este conflicto se conoce como la Guerra en el Este de Ucrania o el conflicto en el Dombás.

La Guerra de Crimea y el conflicto en el este de Ucrania han tenido un impacto duradero en las relaciones internacionales con sanciones impuestas a Rusia por parte de varios países y una continua tensión en la región. La situación en Ucrania sigue siendo un tema de importancia geopolítica en el escenario mundial, dado que el conflicto aún sigue en desarrollo.

2.2 Objetivos Operacionales de la Federación Rusa

Kenny, Locatelli, y Zarza (2015, p. 61) establecen que, “el objetivo es el elemento primordial de cualquier diseño o planificación militar”. A su vez, determinan que deben establecerse objetivos en todos los niveles de la conducción.

> En una situación dada, caracterizada por intereses encontrados, puede surgir la opción militar. A medida que dicha opción se va desarrollando en función de una directiva política, surgirá la cadena de objetivos. En los niveles político y estratégico, los objetivos se denominan como tales; análogamente en el nivel estratégico militar, se denomina objetivo estratégico militar (OEM), en el nivel operacional, objetivo operacional y en el nivel táctico, objetivo táctico (OT) (Kenny, Locatelli, & Zarza, 2015, p. 61).

El proyecto de reglamento, Planeamiento para la Acción Militar Conjunta año 2023 establece que:

> Un objetivo debe ser definido claramente, ser decisivo y ser alcanzable. El planeamiento conjunto debe integrar las capacidades y acciones militares en tiempo, espacio y propósito con otros instrumentos del poder nacional para proveer una unidad de esfuerzos orientada al logro de los objetivos militares del Comandante Operacional. Estos Objetivos Operacionales (OO), a su vez, contribuyen al logro de los Objetivos Nacionales. Los objetivos, y los efectos relacionados, proveen las bases para identificar tareas a ejecutar. En el proceso de planeamiento, son los Objetivos (y sus condiciones o efectos relacionados), más que el Estado Final Deseado, quienes definen la orientación de las acciones de un Comandante para contribuir con los Objetivos Nacionales (Estado Mayor Conjunto de las Fuerzas Armadas, 2023, c. 2, p. 58).

"Para que la coherencia entre los elementos quede asegurada, en general la misión en el nivel operacional debería quedar conformada por el objetivo operacional que expresa la tarea, en función del objetivo estratégico militar que expresa el propósito" (Kenny, Locatelli, & Zarza, 2015, p. 64).

> […] El objetivo de las operaciones militares de Rusia en Ucrania no es simplemente adquirir territorio -si quisiera, Rusia podría haber fácilmente anexado militarmente al Dombás, la zona de conflicto en el este de Ucrania, por ahora-sino más bien para mantener a Ucrania oprimida, sembrar confusión entre su público y evitar que Ucrania ingrese a instituciones Occidentales. Rusia busca socavar los principios fundamentales de cada institución a la que Ucrania quiere unirse. […] Las operaciones militares rusas en Ucrania son solo un componente para debilitar a Occidente y por extensión, hacer que el mundo sea más multipolar (Vertuli & Loudon, 2018, pp. 73-74).

Para poder establecer cuáles fueron los OO de la FR, se debe tener presente las principales causas que la motivaron a invadir Crimea. Rusia manifestó que sus fronteras, la seguridad de la flota del mar Negro y la población ruso parlante estaban siendo amenazadas, por un proceso de occidentalización sobre los ex países soviéticos por parte de la OTAN. A su vez, sus intereses económicos estaban en riesgo si Ucrania firmaba el tratado de libre comercio con la UE (Rodríguez, 2019, pp. 31-32).

Teniendo en cuenta lo expresado en el proyecto de reglamento (Estado Mayor Conjunto de las Fuerzas Armadas, 2023, c. 2, p. 58) existen cinco consideraciones primarias para definir un objetivo:

- Debe establecer un resultado único.
- Debe estar directa o indirectamente relacionado con otros objetivos de nivel superior o con el estado final militar.
- Debe ser específico e inequívoco.
- Debe incluir un Objetivo Material y un Efecto Deseado.
- No debe implicar medios o métodos, ni estar redactado en forma de tarea.

Tomando como base su definición teórica, sus características particulares y la situación reinante, se infiere que los OO que estableció Rusia para su operación militar en Crimea en el año 2014 fueron los siguientes:

- Controlar la península de Crimea.
- Neutralizar las fuerzas ucranianas en Crimea.
- Asegurar las bases militares y la infraestructura estratégica en la península.
- Proteger a la población prorrusa en la península.
- Legitimar las acciones propias ante la comunidad internacional y nacional.
- Desestabilizar política, social y económicamente el nuevo Gobierno ucraniano.

2.3 Operaciones de Información

Las fuerzas de la FR ejecutaron una campaña de información antes, durante y después de las operaciones militares en Crimea. Su audiencia principal fue el público ruso en propio territorio y la población prorrusa residente en Crimea. Los MCS rusos manipularon la cobertura de los acontecimientos en Crimea para conseguir la aprobación de su población. La campaña incluyó asumir la dirección de los pocos MCS nacionales independientes que quedaban, obteniendo un mayor control y poder, para dar forma a las opiniones en Rusia sobre los eventos en Ucrania. Se interrumpió la transmisión de los canales de televisión ucranianos, permitiendo solo el acceso a los

canales de la FR. Los MCS rusos se referían al Gobierno interino de Ucrania y al movimiento de protesta como una junta fascista (Kofman, y otros, 2017, p. 12).

Rusia ejecutó una campaña de información contra las instituciones ucranianas buscando alcanzar una serie de objetivos claramente definidos: (Kofman, y otros, 2017, p. 13)

- Desacreditar el nuevo Gobierno de Ucrania, afirmando que era ilegítimo y fallido.
- Socavar el apoyo de los manifestantes y facciones Occidentales en Ucrania.
- Provocar temor en la población ruso parlante, manifestando que sería prohibido el idioma ruso en la región.
- Demostrar un amplio apoyo para el regreso de Crimea a la seguridad de Rusia.

La campaña informacional se planificó buscando alcanzar al público blanco, haciendo hincapié en una serie de narrativas con tres focos bien definidos, uno de carácter general y otro sobre el rol del Gobierno ucraniano y por último sobre el rol de los países de Occidente.

Tabla 1

Mensajes de la Estrategia Comunicacional Rusa en Crimea

Carácter General	Rol del Gobierno ucraniano	Rol de los países Occidentales
- El territorio de Crimea históricamente perteneció a Rusia. - La cesión de Crimea a Ucrania en 1954 fue un error histórico del período soviético. - Los ruso-parlantes que habitan en Crimea se encuentran bajo una amenaza inminente de los ucranianos ultranacionalistas. - Rusia no ha participado de los sucesos que se están desarrollando en Crimea. - El referéndum del 16 de marzo fue legítimo y expresó la voluntad del pueblo de Crimea. - Los soldados ucranianos se han rendido voluntariamente y han jurado lealtad a Rusia.	- El Gobierno de Ucrania actúa según los intereses de los EE.UU. y otras potencias extranjeras. - El movimiento Euromaidán es dirigido por ultranacionalistas violentos. - El presidente ucraniano fue derrocado por un golpe de estado ilegítimo respaldado por Occidente. - La población de Ucrania con raíces europeas es descendiente de simpatizantes ideológicos, nazistas y fascistas.	- Los países Occidentales, especialmente EE.UU., son los responsables de los eventos en Ucrania. - La principal motivación de los EE.UU. es la expansión de la OTAN hacia el este para contener a Rusia. - EE.UU. presiona a Europa para que imponga sanciones a Rusia. - La política Rusa no se aparta de las intervenciones Occidentales anteriores para modificar las fronteras y crear nuevas entidades políticas, como en Kosovo.

Nota: Basado en la investigación realizada por la Rand sobre la campaña de información rusa en Crimea (Kofman, y otros, 2017, c. 2, p.14).

Sobre la base de la tabla 1, se establece que la campaña comunicacional rusa utilizó diferentes herramientas para difundir sus mensajes (Kofman, y otros, 2017, pp. 82-83).

2.3.1 Medios de Comunicación Social

- Control de los canales de televisión de Rusia y Ucrania como noticieros, programas de entrevistas, documentales, reportajes especiales, etc.
- Control de páginas de noticias en Internet de Rusia y Ucrania.
- Control de Blogs y RS.
- Control de diarios impresos de Rusia y Ucrania.
- Control de espacios publicitarios durante el referéndum.

2.3.2 Personalidades Afines a los Intereses Rusos

- El presidente Vladmir Putin, el Ministro de Relaciones Exteriores Sergei Lavrov y otros políticos rusos y expertos.
- Políticos y expertos ucranianos afines al Gobierno ruso.
- Organizaciones y partidos políticos prorrusos en Ucrania.
- Políticos y expertos Occidentales de Europa y los EE.UU..
- Líderes de protestas locales y ciudadanos comunes.

2.3.3 Estrategias Narrativas

- Socavando la legitimidad del Gobierno de Ucrania.
- Creando una sensación de amenaza y emergencia.
- Manipulando la memoria y los hechos históricos.
- Manipulando los hechos y brindando información errónea o incompleta.
- Simplificando la realidad buscando generar dudas y ambigüedad.

2.4 Factores de Éxito de la Campaña Informacional

El Kremlin empleó las RS de manera efectiva para generar apoyo interno y difundir noticias con desinformación sobre las protestas de Kiev y las intenciones del nuevo Gobierno. Un análisis de las OI de Rusia en el conflicto ucraniano encontró cinco factores de éxito en su campaña informacional: (Kofman, y otros, 2017, c. 2, p. 28)

- Impacto masivo y duradero, mediante la repetición de los mismos temas.
- Manipulación de la información difundida para crear temor en los prorrusos.
- Agitación emocional, uso de narrativas para que los prorrusos actúen por ira.
- Claridad del mensaje, presentando el conflicto en términos simples.
- Obviedad, hacer coincidir la propaganda con mitos y leyendas rusos.

Otro factor de éxito fue la predisposición del público étnicamente ruso de la región, que se negó a reconocer la legitimidad del Gobierno de Kiev. Un 71.3% de los crimeos consideró que la anexión tendría un impacto positivo para la región. Un público objetivo

receptivo les permitió difundir la narrativa rápidamente entre quienes los apoyaban y al mismo tiempo demonizar a quienes se oponían a la anexión rusa (Holloway, 2017).

2.5. Operaciones de Información Rusas Durante la Invasión a Crimea

> Desde mediados de 2013 Rusia llevó adelante la Operación Armagedón, la cual consistió en una campaña de ciberespionaje dirigida contra el gobierno, las fuerzas policiales y militares ucranianas. Estas acciones acontecieron cuando el gobierno de Yanukovich y la Unión Europea iniciaron las reuniones para el Acuerdo de Asociación. Al iniciarse las protestas contra el gobierno ucraniano, un *malware* llamado Snake infectó la oficina del primer ministro de Ucrania y el de varias embajadas fuera del país. Esta operación ayudó a proporcionar una ventaja militar a Rusia frente a Ucrania a partir de secretos recopilados sistemáticamente del ciberespionaje (Azhar & Shaheen, 2015 como se citó en Belletti, 2021, p. 13).

Durante el conflicto, el Gobierno ruso gastó más de 19 millones de dólares para financiar a 600 personas para que comentaran artículos de noticias, escribieran blogs y operaran en las RS. Su intención era influir en la opinión pública e internacional, acallar las voces de los disidentes y crear una imagen de una población que apoyaba la anexión. Para lograrlo, apelaron a la población prorrusa de Crimea, difundiendo rumores de odio y miedo. Uno de esos rumores involucraba la crucifixión de un niño de tres años en la plaza pública de Slavyansk por soldados ucranianos, pero fuentes independientes rápidamente desacreditaron esta historia (Holloway, 2017).

Según Iasiello (2017), Rusia negó su participación en los ataques hasta las últimas etapas del conflicto, paralelamente expresó su deseo de reducir la escalada de la crisis mientras aumentaba el caos. Ni EE.UU., ni la OTAN o la UE pudieron predecir los objetivos de Rusia, esto le permitió al Kremlin aprovechar el control reflexivo para operar dentro de los bucles de toma de decisiones Occidentales, reduciendo los costos de sus acciones contra Ucrania y manteniendo a los EE.UU. y sus aliados fuera del conflicto. Cuando Putin admitió la presencia de tropas rusas, ya había anexado Crimea.

Moscú utilizó los MCS prorrusos para difundir fotos de tanques, banderas y soldados ucranianos alterados con símbolos nazis para asociar al Gobierno ucraniano con el resurgimiento del nazismo y, por lo tanto, influir en algunos países europeos, como Alemania, para que se distancien de ellos de Kiev. También difundió imágenes que mostraban columnas de refugiados que huían de Ucrania a Rusia, cuando en realidad la gente viajaba diariamente entre Ucrania y Polonia (pp. 56-57).

> El blanco de las OI también fueron los miembros militares de Ucrania combatiendo en primera línea. Poco después de que la lucha comenzará en Ucrania oriental, en 2014, por ejemplo, soldados desplegados a la región de combate comenzaron a recibir "textos falsos". Los mensajes a menudo tenían intención de amenazar y desmoralizar a las tropas en un conflicto "agotador" con algunos textos en los que se leía: "Soldados ucranianos, encontrarán sus cuerpos cuando la nieve se derrita"; "Vete y vivirás"; "Nadie necesita que tus hijos se conviertan en huérfanos"; "Soldado ucraniano, es mejor retirarse vivo que quedarse aquí y morir" y "No recuperarás a Dombás, más derramamiento de sangre no tiene sentido" (Vertuli & Loudon, 2018, p. 76).

Las Fuerzas Rusas también enviaron mensajes con el objetivo de afectar la cohesión y la moral de la unidad. Los textos simulaban ser enviados por propios camaradas afirmando que su comandante había desertado o que las fuerzas ucranianas estaban siendo diezmadas y que deberían huir (Vertuli & Loudon, 2018, p. 76).

Rusia combinó OI con operaciones cinéticas, su táctica iniciaba con un mensaje de texto a un soldado, diciéndole que estaba rodeado y abandonado. Más tarde, la familia recibía un mensaje de texto diciendo, su hijo había muerto en acción. La familia llamaba para corroborar si la noticia era cierta. Luego del mensaje de texto inicial, el soldado recibía otro mensaje, retírate y vivirás. Posteriormente, la artillería rusa ejecutaba un ataque, sobre la ubicación donde se había detectado un gran grupo de teléfonos celulares destinatarios. Así, en una acción coordinada, utilizó OI para intimidar al soldado y su familia y combinó esto con guerra electrónica y fuego de artillería para producir efectos tanto cinéticos como psicológicos (Vertuli & Loudon, 2018, p. 77).

2.6 Consideraciones Finales del Capítulo

A lo largo del segundo capítulo se han abordado diversos aspectos relacionados con el conflicto en Crimea en 2014, enumerando las causas que dieron origen al conflicto y cuáles podrían haber sido los OO de las Fuerzas Rusas. Seguidamente, se analizó la campaña informacional ejecutada antes, durante y después de las operaciones militares y se describieron las narrativas que utilizaron y a qué blanco fueron dirigidas para contribuir con el cumplimiento de los objetivos planteados. Por último, se mencionaron diferentes tipos de OI que se ejecutaron durante el conflicto, quedando claro que Rusia llevó a cabo una serie de OI complejas y coordinadas buscando influenciar al enemigo y la población con el objetivo principal de anexar la península de Crimea a la FR.

Conclusiones

De lo analizado durante el presente trabajo final integrador surge que, en los últimos años, se ha producido un cambio drástico en el caracter de la guerra y, por lo tanto, aquellas naciones que no se adapten al nuevo paradigma corren el riesgo de no estar preparadas para los futuros conflictos.

En los enfrentamientos modernos, se observa que, los contendientes evitan el combate directo, dado que conlleva significativos costos en recursos materiales y vidas humanas. Ante estas nuevas reglas de juego, los países involucrados se esfuerzan por influir sobre la percepción de la población enemiga con el objetivo de obtener ventajas estratégicas mediante diversas presiones que afecten las decisiones de sus líderes.

Las funciones conjuntas han surgido en la doctrina como una forma de expresar aquellas dimensiones del conflicto donde la combinación de instrumentos de poder es especialmente útil. Por esta razón, las OI deben considerarse como una función conjunta, ya que sus efectos son transversales a todas las FFAA y deben ejecutarse mediante un planeamiento centralizado en el Teatro de Operaciones. Dada su naturaleza inmediata, su alcance global y su difusión constante, la información posee la capacidad de comprimir los niveles de la guerra al existir una mayor cantidad y calidad disponible. Estas características particulares permiten simplificar el proceso de toma de decisiones y reducir el tiempo de respuesta en situaciones de crisis y conflictos armados.

Esta función conjunta abarca la gestión y difusión de la información para cambiar o mantener percepciones, actitudes y otros conductores del comportamiento, para apoyar la toma de decisiones humana. Es la organización intelectual de las tareas necesarias para utilizar la información durante todas las operaciones y comprender cómo afecta el ambiente operacional.

Rusia ha ejecutado OI, desde la Guerra Fría hasta la era digital, utilizando tanto la *maskirovka* como la *spetspropaganda* para influir en la percepción pública, como parte de su estrategia política y militar. Posee gran experiencia en el desarrollo de OI, obtenida luego de haberlas aplicado con éxito en los conflictos de Estonia 2007, Georgia 2008 y Crimea 2014. Estos combates consolidaron su posición de referente mundial en esta área, respaldando la doctrina elaborada por Gerasimov, la cual sostiene que la naturaleza de la guerra ha evolucionado y que Rusia ha sabido adaptarse a estos cambios.

A diferencia de las potencias Occidentales, Rusia tiene un enfoque holístico y multidisciplinario de las OI. Abarcando diferentes áreas, desde lo político y lo militar

hasta lo económico y lo tecnológico. Esta visión integral le permite a Rusia ejecutar OI en tiempos de paz y de guerra para alcanzar sus objetivos estratégicos y operacionales.

Las tropas de OI rusas, han sabido integrar hábilmente técnicas de manipulación de información, espionaje, interferencia política, engaño militar y manipulación de RS para influir y desestabilizar a los países extranjeros. Esta estructura operativa dificulta la capacidad para contrarrestar eficazmente estas operaciones a las naciones afectadas que no tienen su propio sistema de OI, representando un desafío para su seguridad.

La invasión de la península de Crimea brindó una oportunidad para confirmar que las OI son un arma efectiva en los complejos ambientes operacionales actuales. En este escenario específico, Rusia logró aislar la región de las noticias del mundo exterior y sus tropas de OI fueron capaces de combinar acciones físicas y de información para manipular las noticias e influenciar la audiencia interna y externa.

Crimea sirvió como campo de prueba para las OI rusas, donde demostró al mundo la eficacia de las RS como sistema de armas en el ámbito informacional, ya que incitando a la población prorrusa, logró anexar el territorio de otra nación soberana sin el empleo de fuerzas convencionales. Las acciones rusas permiten concluir que el empleo de las RS es esencial para dar forma a la narrativa de las OI, y que si se utilizan los tiempos, los mensajes y el público blanco adecuado, las RS son capaces de manipular el resultado de un conflicto. Por lo tanto, se deben prever las medidas para accionar contra esta amenaza y emplearlas a nuestro favor mediante la capacitación.

Quedó demostrado que, ante la ausencia de una amenaza militar directa, Rusia utilizó recursos no militares como la propaganda, la desinformación, la negación y el engaño para influir en las diferentes audiencias. Utilizó los programas televisivos para generar apoyo de sus acciones en Crimea y reforzar la idea que buscaban proteger a los rusos parlantes de la península. Los MCS prorrusos comunicaron narrativas falsas sobre hechos reales, como negar la presencia del ejército ruso en Ucrania o culpar a Occidente por llevar a cabo un desprestigio contra Rusia para tratar de legitimar sus acciones.

A través de la estrategia de socavar la moral del enemigo y sus familias mediante el envío de mensajes de texto, alentando la deserción de sus puestos de combates, las fuerzas rusas lograron debilitar la resistencia enemiga, neutralizar las fuerzas ucranianas casi sin oposición y finalmente controlar la península de Crimea.

Los mensajes dirigidos a los rebeldes los mantuvieron comprometidos en la lucha, mientras que los mensajes a la población nacional crearon una justificación moral para apoyar a los rebeldes. Rusia utilizó la narrativa de proteger a la población rusa en Crimea

como justificación para su intervención. Las OI contribuyeron a crear un ambiente en el que esta población se sintiera apoyada y protegida por Rusia, facilitando la anexión.

Las OI rusas crearon división y desconfianza en el nuevo Gobierno ucraniano, especialmente al tratarlo como ilegítimo y asociado con grupos extremistas. Esto generó tensiones políticas, sociales y económicas en Ucrania, lo que desestabilizó al país y dificultó su respuesta a la anexión de Crimea.

Otra lección aprendida de la anexión de Crimea es que las OI deben incorporarse al proceso de planeamiento de comando. Si bien las tropas de OI tienen en cuenta sus efectos y buscan difundir la narrativa planificada durante las operaciones, las fuerzas convencionales no emplean estos recursos para influir eficazmente en la población. Para contrarrestar esta deficiencia, la cadena de comando debe permitir y alentar a las unidades subordinadas capturar datos, fotografías o videos, del campo de batalla para utilizarlos en caso de ser necesario en el dominio informacional. Las tropas equipadas con cámaras en el combate pueden contrarrestar las OI del enemigo.

Es necesario que las tropas comprendan que en la actualidad hay millones de ojos puestos sobre ellos, sus acciones y los movimientos de las fuerzas son observados constantemente por el enemigo y la población civil, cualquier error puede convertirse en una noticia de alto impacto que se difunde rápidamente a través de las RS. En los entornos actuales, todos los integrantes de las fuerzas armadas tienen la responsabilidad de tomar la decisión correcta en el momento adecuado para evitar convertirse en el cabo estratégico que los acerque a la derrota.

Para concluir, en este trabajo se utilizó el caso histórico de Crimea 2014 para analizar las OI que realizó un país referente en la materia. A lo largo del mismo se ha podido ilustrar, a través de ejemplos concretos, como una campaña comunicacional llevada a cabo de manera estratégica, haciendo uso de una amplia variedad de recursos y tácticas en múltiples operaciones cuidadosamente ejecutadas, desempeñaron un papel fundamental en el logro de gran parte de los OO establecidos. En consecuencia, este trabajo ha contribuido significativamente a nuestra comprensión de cómo las OI pueden contribuir al logro de los objetivos impuestos en el nivel operacional.

Las conclusiones expuestas, en consonancia con los objetivos específicos planteados, permiten considerar que el objetivo general del trabajo final integrador ha sido alcanzado.

Bibliografía

Belletti, F. (2021). *Las operaciones de ciberguerra y su contribución al logro de los objetivos del nivel operacional: caso de estudio el accionar de Rusia contra Ucrania.* CABA: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Bilibio, R. M. (2017). *La importancia de la aplicación de las operaciones de información en un ambiente operacional.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Bilyana, L., & Cheravith, J. (2020). The past, present and future of Russia´s cyber strategy and forces [El pasado, presente y futuro de las fuerzas y ciber estratégias Rusas]. En *12th International Conference on Cyber Conflict [12mo Conferencia Internacional sobre conflictos ciberneticos]* (págs. 129 - 155). Estonia: NATO CCDCOE Publications.

Cheravitch, J. (2021). *The Role of Russia's Military in Information Confrontation [El papel del Ejército Ruso en la Confrontación de Información].* Obtenido de https://www.cna.org/reports/2021/06/The-Role-of-Russia%27s-Military-in-Information-Confrontation.pdf

Cockrell, C. (2018). Los métodos y las acciones Rusas contra los Estados Unidos y la OTAN. *Military Review.*

Darckzewska , J. (2014). *The anatomy of Russian information warfare [La anatomia de la guerra de la información de Rusia].* Warsaw, poland: Orodek studiów wschodnich.

de Vergara, E., & Trama, G. A. (2016). *Operaciones militares cibernéticas.* Visión Conjunta.

Department of the Navy. (2022). *Marine Corps Doctrinal Publication 8 Information [Publicación Doctrinal del Cuerpo de Marina 8 Información].* Washington: U.S. Marine Corps.

Estado Mayor Conjunto de las Fuerzas Armadas. (2019). *Glosario de términos de empleo militar para la acción militar conjunta.* Ministerio de Defensa.

Estado Mayor Conjunto de las Fuerzas Armadas. (2023). *Planeamiento para la Acción Militar Conjunta* . Buenos Aires: Ministerio de Defensa.

Ferrari, Vigón, Gaggero. (2001). *Curso de Formación de Oficial de Estado Mayor.* Argentina: Escuela Superior de Guerra Teniente General Luis María Campos.

Gerasimov, V. (2013). “Ценность науки в предвидении” [El valor de la ciencia está en la previsión]. *Voienno-Promyshlenny Kurier*.

Gerasimov, V. (2016). The value of science is in the foresight (R. Coalson, Trans) [El valor de la ciencia está en la previsión] (Trabajo original publicado en 2013). *Military Review.*

Gómez Arriagada, H. (2015). *INFOOPS, el ocaso de una moda.* Revismar.

Hassan, M. E. (2019). A 5 años de la anexión de Crimea a Rusia. *Instituto de Relaciones Internacionales.*

Holloway, M. (10 de Octubre de 2017). *The Strategy Bridge [El Puente Estratégico]*. Obtenido de How Russia Weaponized Social Media in Crimea [Como Rusia utilizó las redes sociales como armas en Crimea]: https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea

Iasiello, J. (2017). *Russia's Improved Information Operations: From Georgia to Crimea [Mejoras en las operaciones de información de Rusia: de Georgia a Crimea]*. USAWC.

Iglesisas Sanchez, O. I. (2021). *Operaciones de Rusia en zona gris: Fundamentos y desarrollo en su inmediata periferia europea.* Madrid: Instituto Universitario General Gutiérrez Mellado.

Jaitner, M., & Mattsson, P. (2015). Russian Information Warfare of 2014 [Guerra de Información Rusa en 2014]. En M. Maybaun, & A. Osula, *Architectures in Ciberspace [Arquitecturas en el Ciberespacio]* (pág. 39). Tallinn, Estonia: NATO CCD COE.

Kenny, A., Locatelli, O., & Zarza , L. (2015). *Arte y diseño operacional, una forma de pensar opciones militares.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., & Oberholtzer, J. (2017). *Lessons from Russia’s operations in Crimea and eastern Ukraine [Lecciones de las operaciones rusas en Crimea y el este de Ucrania]*. California: RAND Corporation.

Makotczenko, M. (2019). *Una nueva visión de la estrategia militar en la concepción del General de la Federación Rusa, Valery Gerasimoc.* CABA: Visión Conjunta.

Mc Guinness, D. (06 de 05 de 2017). *BBC News Mundo.* Obtenido de Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país.: https://www.bbc.com/mundo/noticias-39800133

Michelle Grisé, A. D. (2022). *Rivalry in the Information Sphere [Rivalidad en la esfera de la información]*. California: RAND. Obtenido de https://www.rand.org/pubs/research_reports/RRA198-8.html

Motta, G. L. (2023). La teoría de la innovación militar: el caso de la inteligencia táctica del Ejército Argentino (2008-2017). *Revista de la Escuela Nacional de Inteligencia*, 13-33.

Pipes, R. (1995). *A concice history of the Russian Revolution [Una historia concisa de la Revolución Rusa]*. New York: Knopf.

Poder Ejecutivo Nacional. (2021). *Directiva de Política de Defensa Nacional.* CABA.

Policante, O. A. (2019). *El desarrollo de operaciones interagenciales dentro del nivel operacional en un contexto de guerra híbrida en el conflicto de Ucrania durante el 2014.* CABA: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Putin, V. (2000). *Доктрина информационной безопасности Российской Федерации [Doctrina de seguridad de la información de la Federación Rusa]*. Moscu: Decreto Presidencial del Gobierno de la Federación Rusa.

Real Academia Española. (2022). *Real Academia Española.* Obtenido de https://dle.rae.es

Rodriguez, R. R. (2019). *La dificultad de identificar el centro de gravedad en la guerra híbrida.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Snegovaya, M. (2015). *Putin´s information warfare in Ukraine [La guerra de la información de Putin en Ucrania]*. Washington: Institute for the Study of War.

Stel, E. (2005). *Guerra Cibernética.* CABA: Círculo Militar.

Vertuli, M., & Loudon, B. (2018). *Percepciones son realidad.* EE.UU.: Prensa de la Universidad del Ejército.

Wilde, G., & Sherman, J. (04 de Enero de 2023). *Carnegie Endowment*. Obtenido de No Water's Edge: Russia's Information War and Regime Security [La guerra de información de Rusia y la seguridad del régimen]: https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-

88644#:~:text=The%202000%20Information%20Security%20Doctrine,the%20state%20of%20the%20protection

Tabla de Abreviaturas

DPDN: Directiva de Política de Defensa Nacional.

EE.UU.: Estados Unidos de América.

FFAA: Fuerzas Armadas.

FR: Federación de Rusia.

KGB: del Ruso, Comité para la Seguridad del Estado.

MCS: Medios de Comunicación Social.

OEM: Objetivo Estratégico Militar.

OI: Operaciones de Información.

OO: Objetivo Operacional.

OT: Objetivo Táctico.

OTAN: Organización del Tratado Atlántico Norte.

RS: Redes Sociales.

TIC: Tecnologías de la Información y las Comunicaciones.

UE: Unión Europea.

URSS: Unión de Repúblicas Socialistas Soviéticas.

.