MATERIA:

TALLER DE TRABAJO FINAL INTEGRADOR

TEMA:

Operaciones de Información – Implementación Doctrinaria y Experimentación en el Nivel Operacional

TÍTULO:

Las Operaciones de Información en el Conflicto Rusia - Ucrania

AUTOR: MY EDUARDO JOSE PAVAN ECHAVARRIA

ASESOR: CORONEL MARIO ALFONSO

Año 2022

Resumen

El conflicto entre Rusia y Ucrania, se remonta desde tiempo de antaño, siendo Ucrania un país con una estrecha vinculación a Rusia. Así mismo nos centraremos desde la crisis del año 2014, en la disputa de la Península de Crimea hasta febrero del año 2022 donde el conflicto pasa a tener vigencia plena, luego de la invasión por parte de Rusia.

Estos dos países, por un lado Ucrania que negocia su incorporación a la Unión Europea como así también a la Organización del Tratado del Atlántico Norte, y por otro lado, Rusia que no quiere la independencia de Kiev y tampoco la incorporación a los organismos internacionales anteriormente nombrados, tienen diferentes intereses y los dos velan por el cumplimiento de los mismos.

El avance de la tecnología en el mundo y su rápida disipación en todos los ámbitos ha provocado que quien este exento de la misma corra en desventaja de acuerdo a sus intereses, y que quien las maneje y domine obtendrá una ventaja cuantiosa, y de esta forma tendrá mayor posibilidad de obtener la victoria ya sea antes, durante el transcurso o después del conflicto.

Estas posibles operaciones de información son el motivo de la presente investigación, para tomar como ejemplo de un conflicto actual y ante la realidad de las Fuerzas Armadas Argentinas, las cuales no cuentan con capacidades para operar la guerra de la información.

La doctrina Argentina vigente contempla la guerra de la información, pero no especifica cuales son las operaciones a desarrollar, ni tampoco sienta las bases para el desarrollo de una doctrina derivada de este tipo de guerra.

1. Palabras Clave

Información – Operacional – Conflicto – Rusia – Ucrania.

Índice de contenido

Introducción

El conflicto entre Rusia y Ucrania es fruto de muchos factores que fueron madurando en el tiempo, se remonta desde sus inicios pasando por la anexión de Crimea a Rusia en el año 2014 hasta el presente, en donde se puede observar el desarrollo del conflicto armado en toda su expresión. Rusia busca como fin la no incorporación de Ucrania como miembro de la Organización del Tratado del Atlántico Norte como así también a la Unión Europea.

Esta posible incorporación de Ucrania a las organizaciones anteriormente nombradas, Rusia lo toma como una amenaza, ya que si Ucrania lograra su cometido, Rusia perdería el espacio de amortiguación existente con la Unión Europea, como así también con la Organización del Tratado del Atlántico Norte, en donde Estados Unidos es el integrante más importante y al cual Rusia no quiere en sus fronteras. Esta amenaza llevó a que Vladimir Putin tomara la decisión de iniciar la operación especial en Ucrania, empleando todo el poder militar para mantener y ampliar esa zona de amortiguación y demostrar su estatus de potencia en Eurasia.

Hoy en día las nuevas tecnologías cambian la forma de comunicación en los seres humanos, esto no deja de lado a los conflictos armados, que también deben adaptarse para evolucionar y estar a la altura de los cambios. Desde la Segunda Guerra Mundial en adelante la tecnología ha impuesto que antes, durante un conflicto y luego del mismo, se utilicen estas nuevas herramientas para favorecer a quienes las empleen y darles una ventaja cuantiosa y eficaz para poder lograr los objetivos.

Estas nuevas herramientas o avances tecnológicos llevarán a que el comandante deba anticiparse en la toma de decisiones, para crear las condiciones necesarias y poder desarrollar operaciones eficaces y lograr los objetivos que se hayan impuesto. Es así que las operaciones de información, que hoy en día están en auge, contribuyen en la toma de decisiones y son parte fundamental de la campaña.

El desafío de hoy que tienen los estados y sus fuerzas armadas, es generar y mantener las capacidades necesarias para poder aprovecharlas, como también para poder afrontar y repeler las acciones por parte del enemigo.

Los conflictos se desarrollan por motivos e intereses que disputan los diferentes actores que están involucrados. Estos actores, estados o países van a desarrollar sus campañas militares y estas van a estar encuadradas por factores que le van a dar forma para lograr un objetivo operacional y así poder contribuir al logro del estado final operacional deseado.

En los conflictos actuales las campañas no pueden dejar de lado, ya sea al momento del planeamiento y diseño, al momento de la ejecución o al momento de la finalización de la misma, un elemento fundamental e imprescindible como es el manejo de la información.

Este manejo y control de la información es fundamental para toda campaña, ya que puede ser la mejor arma para el logro de los objetivos de la misma. Esto obliga a los líderes o conductores militares a desarrollar estrategias comunicacionales para llevar a cabo las operaciones de información que contribuyan a la campaña.

Las estrategias comunicacionales que se deberán planificar las podemos definir como:

> Modelo o plan que integra los principales objetivos, políticas y sucesión de acciones, para el óptimo y eficiente empleo de los recursos disponibles buscando hacer común una idea, una situación, o una intención en oportunidad, donde el responsable primario de esta área es la figura y asesor oportuno para que el decisor adopte una resolución pertinente y efectiva de acuerdo al contexto y contingencia en la que se encuentra la institución. (Keller, Cuello & Tabbia, 2004, p. 43).

En la doctrina de los Estados Unidos de América, se encuentra el desarrollo del concepto de operaciones de información, siendo el mismo el siguiente:

> Operaciones de Información (IO) es el empleo integrado, durante operaciones militares, de capacidades relacionadas con la información en conjunto con otras líneas de operación para influenciar, interrumpir, corromper o usurpar la toma de decisiones de adversarios y adversarios potenciales mientras protegemos la nuestra (JP 3-13). (Ejército de Estados Unidos, FM 3-13, 2016)

En la doctrina del ejército del Brasil, se encuentra el desarrollo del concepto de las operaciones de información, siendo el siguiente:

> Las Operaciones de Información (Op Info) consisten en actuar metodológicamente mediante capacidades integradas y relacionadas con la información y con otros vectores, consisten en informar, influir en grupos e individuos, así como afectar el ciclo de toma de decisiones de oponentes, mientras protegemos a los nuestros. Además, tienen como objetivo evitar, prevenir o neutralizar los efectos de acciones adversas en la Dimensión Informativa. (Ejército de Brasil, 2014, p. 3-1).

En la doctrina de ejército de Chile, podemos encontrar el desarrollo del concepto de operaciones de información, siendo el mismo el siguiente:

> Las operaciones de información se definen como el conjunto de acciones coordinadas que se realizan para influir en la toma de decisiones de un adversario en apoyo de la consecución de los objetivos propios, influyendo en

> su capacidad para explotar y proteger la información, en los sistemas de mando y control que la soportan y en los sistemas de telecomunicaciones e información que la procesan, mientras se resguardan los propios. (Ejército de Chile, 2010, p. 17)

Entre otras definiciones de operaciones de información, se destaca la siguiente:

"Una operación de información es una función militar para proporcionar asesoramiento y coordinación a las actividades militares de información para crear los efectos deseados en la voluntad, entendimiento y capacidad del adversario, potenciales adversarios y otros actores" (Bilibio, 2017, p. 13).

Las operaciones de información el siguiente autor las define como "Son acciones tomadas para afectar e influir los procesos de toma de decisiones, información, y sistemas de información del adversario y otras entidades mientras que se protege su propia información y sistemas de información" (Campos, 2021).

De estas definiciones anteriormente nombradas se desprenden las operaciones que proporcionan el núcleo de la Guerra de la Información que son:

a. Ciberwar (Arquila, Ronfeldt, 1993)
b. Netwar (Arquila, Ronfeldt, 2001)
c. Swarming (Arquila, Ronfeldt, 2001) (Campos, 2021).

Cuando se analiza nuestra doctrina la Guerra de la Información se la nombra pero no se profundiza en la misma, se la menciona como tal en el ROB 00-01 "Conducción de la Fuerzas Terrestres" en el Cap II Las Fuerzas Terrestres, en la Sec II Funciones de Combate y en su art. 2009 Inteligencia, definiéndola, y en el Cap VII Operaciones Complementarías en sus Secciones VIII Guerra Electrónica, IX COSACO y XV Ciberdefensa, dentro de sus características aclaran que:

> "(…) integran el conjunto de las operaciones que conforman la Guerra de la Información, contribuyendo a la obtención de los objetivos / finalidad que persigue la misma" (Ejército Argentino, 2015, p. 27).

Además de lo anteriormente desarrollado se puede definir de diferentes formas a la guerra de la información, para ello se destacan las siguientes definiciones:

> Guerra de la Información es el uso y manejo de la información con el objetivo de conseguir una ventaja decisiva sobre el enemigo, pudiendo abarcar tanto la obtención de información táctica y la confirmación de su veracidad, como la desinformación, a efectos de afectar las operaciones del enemigo, socavando la calidad de información obtenida por éste y negándole la oportunidad de búsqueda y reunión de información. (Ejército Argentino,

2015, p. 8)

También hay autores que conceptualizan de la siguiente manera:

> Guerra de la Información consiste en el uso ofensivo y defensivo de la información y de los sistemas de información para negar, explorar, corromper o destruir la información del adversario, su proceso de información, los sistemas de información y las redes de computación mientras se procura la protección de los propios sistemas. (Ferrari, Vigón & Gaggero, 2001, p. 35)
>
> Son las acciones que se llevan a cabo para obtener la superioridad en todo lo que afecta a la información, así también como a su procesamiento, sus sistemas de información y protección de las redes de computación propias y de las acciones del adversario. (Ferrari, Vigón & Gaggero, 2001, p. 35)

Estas operaciones de información se encuentran y se ejecutan dentro del ambiente informacional, que puede ser definido como "la sumatoria de individuos, organizaciones y sistemas que obtienen, procesan, difunden o actúan sobre la información" (Spretz, 2018).

Este entorno en donde se ejecutan las operaciones de información comprende tres dimensiones interrelacionadas que interactúan con individuos, sistemas y organizaciones. Una es la dimensión física, compuesta por el comando y control, aquello tangible y real, la otra es la dimensión informativa que comprende la información y el flujo de la misma y la última es la dimensión cognitiva centrada en la mente humana, en los valores, en las creencias, conciencia, toma de decisiones y en las percepciones. Estos factores insertos en la sociedad, política, cultura, religión, etc. accionan sobre las percepciones de quienes producen la información y sobre el público que la recibe. (Spretz, 2018, p. 10-11)

Centrándonos en el conflicto, Rusia aparentemente ha empleado para alcanzar sus objetivos políticos, una mezcla de operaciones especiales, presión económica, agentes de inteligencia, instrumentalización del flujo de gas natural, ciberataques, guerra de información y empleo de fuerza militar convencional como medida de presión y disuasión. Todo ello, perfectamente sincronizado formando parte de un plan de operaciones el cual se puede enmarcar dentro del concepto de guerra híbrida. (Sánchez Herraes, 2014, p. 2)

Continuando con el autor citado explica que, la crisis de Crimea y Ucrania constituye el punto de inicio que desencadena una situación entre Rusia y Occidente que se va complicando de tal forma que comienza a proliferar la idea de encontrarnos en el marco de una Nueva Guerra Fría. (Sánchez Herraes, 2015, p. 1)

La crisis en Ucrania fue desencadenada tras las manifestaciones y altercados violentos generados a raíz de los hechos conocidos como Euromaidán, en noviembre de 2013, el

activador de estos disturbios fue la decisión tomada por parte del Presidente Viktor Yanukovich de posponer la firma del Acuerdo de Asociación y Libre Comercio con la Unión Europea. Esta situación fue tan compleja que los manifestantes, entre los cuales había grupos bien organizados, comienzan a asumir el control del país, es así que el presidente ucraniano prorruso el 22 de febrero del 2014 alega que se estaba ejecutando un golpe de estado para derrocarlo del poder. (Sánchez Herraes, 2015, p. 3)

Ucrania comenzaba a recuperar la calma y a preparar un proceso electoral para elegir nuevo presidente, pero en menos de un mes, empleando lo que se llama guerra híbrida, Crimea y Sebastopol se anexan a Rusia y comienza una insurrección armada en las regiones de Donetsk y Lugansk que el gobierno de Kiev no puede contener, mientras tanto las sospechas y acusaciones hacia Rusia y sus intervenciones ocultas son cada vez más contundentes y constantes. (Sánchez Herraes, 2015, p. 3)

El 31 de diciembre de 2015 Rusia da inicio a su nueva Estrategia de Seguridad Nacional, en la que se establece que el rol de la fuerzas en las relaciones internacionales no ha declinado, si bien Rusia, contempla el empleo de la fuerza militar para proteger los intereses nacionales cuando las medidas de naturaleza no violentas, sean ineficaces.

Esta estrategia de seguridad nacional muestra también que se va a mejorar la organización militar del Estado a través del desarrollo de los elementos de la organización militar, del aumento de las capacidades de defensa y del equipamiento de las Fuerzas Armadas Rusas con armas modernas y hardware especializado, y con algo tan importante como el desarrollo industrial de la defensa basada en la innovación.

La anexión a Rusia de Crimea y Sebastopol (2014), el apoyo a rebeldes en Donestsk y Lugansk (2014) ponen de manifiesto que el empleo de la fuerza militar, de la herramienta militar, continúa siendo una realidad para la Federación Rusa. (Sánchez Herraes, 2016, p. 2)

Todos estos cambios que se fueron dando, no son por casualidad sino porque Rusia mantiene vigente defender sus intereses al costo que sea necesario. Es así que le dan gran relevancia a las operaciones de información para hacer la guerra de la información siendo fundamental para lograr sus intereses.

Las elecciones presidenciales y parlamentarias de Ucrania, de marzo y octubre de 2019, representaron un hito en la historia del país. Fueron la segunda serie de elecciones tras las celebradas en 2014, después de la llamada Revolución de la Dignidad del Maidan, en un momento en que persiste el conflicto con Rusia, y después de que la Unión Europea (UE) y Ucrania hayan firmado un acuerdo de asociación, que permitió una mayor integración a la Unión Europea. Ucrania al ganar las elecciones nuevamente, y por segunda vez los reformistas,

paso la prueba de dos vueltas de las que hablaba Samuel Huntington que se refería a las elecciones que cambian gobiernos sin desmoronar el orden democrático. Dos elecciones consecutivas ganadas llevarían a Ucrania hasta 2024 con un mismo modelo político, y la situarían en un camino sin vueltas atrás de integración a Europa y saldría de la esfera de influencia rusa, el famoso Russkiy Mir, el mundo ruso, llamado así por ellos. (Márquez de la Rubia, 2019, p. 3)

En Ucrania el sentimiento antieuropeo era bajo y desde la anexión de Crimea a Rusia en el año 2014, cayo de manera drástica. Los Ucranianos comenzaron a ver a Europa con otros ojos y con más interés.

En el año 2015, la Unión Económica Euroasiática que era dominada así por Rusia tenía una visión totalmente contraria a la Unión Europea, el apoyo popular hacia esta unión se redujo de manera considerable luego de las agresiones militares por parte de Rusia. Es así que tuvo un 70 por ciento de oposición en Ucrania incluyendo más de la mitad de los rusos parlantes. De esta manera el nacionalismo ucraniano que estaba presente en los partidos políticos, no tenía la intención de ir en contra de la integración con la Unión Europea, que como se sabe eran y son totalmente pro Organización del Tratado del Atlántico Norte por ende pro estadounidenses. (Márquez de la Rubia, 2019, p. 7)

Para la mayoría de los ucranianos la amenaza a su soberanía procedía de Rusia. El freno de la influencia rusa se refleja y es visto en la juventud ucraniana, que creían que el conflicto era permanente entre Rusia y Ucrania. Se manifestaba de forma generalizada la adopción por parte de Ucrania al modelo Ruso por cuestiones como la agresión, la crueldad y la dictadura.

El entonces gobierno de Ucrania mantenía la posición de que iba a retomar el control del Donbass y de Crimea. Era un objetivo nacional altamente popular, sin embargo, era muy poco probable que Rusia devuelva Crimea, y Ucrania por otro lado, nunca había demostrado ninguna actitud de querer luchar por ella.

Para Rusia una solución era que Donetsk y Lugansk se volvieran a unir a Ucrania, pero con un alto grado de autonomía y con un liderazgo político controlado desde el Kremlin. De esta forma Rusia buscaba la federalización de Ucrania, en donde las regiones tuvieran amplios poderes de veto sobre las políticas internas y externas del país, incluyendo el poder de bloquear y negar la adhesión de Ucrania a la Organización del Tratado del Atlántico Norte y a la Unión Europea. Esto proporcionaría a Rusia una forma directa y legal de influir en la política ucraniana, siendo esto considerado una potencial amenaza a su soberanía por los ucranianos. (Márquez de la Rubia, 2019, p. 10)

A Rusia le es cómodo y está satisfecha con un conflicto en el cual puede aumentar o reducir el nivel del mismo cuando lo desee, sin tener que asumir oficialmente ninguna responsabilidad por los resultados, alegando que el Donetsk y Lugansk son regiones separatistas de Ucrania sobre las que Rusia no tiene control.

La flexibilidad para el acuerdo no parece existir entre Rusia, Ucrania y Occidente sobre principios o territorio. Ya que la posición de Rusia es requerirle a Occidente que acepte una división territorial para establecer una zona de amortiguación o esfera de influencia rusa. Y no negociar la devolución de Crimea. (Márquez de la Rubia, 2019, p. 11)

En el transcurso del siglo actual, la evolución de los conflictos entre este y oeste ha vuelto a situar a Ucrania en su posición histórica de territorio fronterizo de Rusia con occidente. De esta forma chocan dos mundos con enfoques totalmente opuestos y en donde los únicos perjudicados son los Ucranianos. Estas dos visiones contrapuestas, por un lado Estados Unidos, como líder la Organización del Tratado del Atlántico Norte, protege los principios que han guiado a las naciones occidentales desde el final de la Guerra Fría, mientras que el Kremlin tiene una perspectiva típicamente geopolítica que defiende intereses percibidos como vitales, como también arraigados sentimientos de identidad nacional. (Pardo de Satanyana, 2021)

Del estudio y análisis de este conflicto cabe destacar que Ucrania debía permanecer neutral respecto a sus intereses de ingresar a la Organización del Tratado del Atlántico Norte y a la Unión Europea y su posicionamiento internacional, frente a los intereses y estrategias de Occidente (Estados Unidos y Unión Europea) y Rusia. (Leimete, 2019)

También se puede afirmar que la posible aceptación de Ucrania en la Organización del Tratado del Atlántico Norte era vista como una manifestación de poder de los Estados Unidos de América y así minimizar y debilitar a Rusia. (Pardo de Santayana, 2021, p. 3)

La evolución de la guerra y la transformación de la misma contribuyó a que la doctrina Rusa particularmente la generada por el General Gerasimov, evolucione hacia las amenazas hibridas y su modo de emplearlas mediante los medios militares y civiles para poder así moverse con comodidad en los nuevos dominios, como el ciberespacio y la información, y así lograr sus objetivos. (Colom, 2018)

De esta manera vemos como Rusia a través de factores sociales y de los medios de información va afectando con sus propias operaciones a los ucranianos, en la denominada zona gris, logrando perfeccionar e intensificar sus tácticas y procedimientos en este dominio, provocando así un agotamiento gradual de la resistencia física y moral del oponente. (Erickson, 2022)

Se transcurre en la era de la información y la guerra sigue siendo un instrumento de la política que le da poder, en donde un estado quiere imponer su voluntad sobre otros. Esta imposición, hace un tiempo no muy lejano eran actos sangrientos o con grandes secuelas para los actores involucrados, hoy en día resulta un juego de actores e intereses en el que el control de la información de todo tipo se ha convertido, más que nunca, en un activo estratégico en sí mismo. (Quiñones de la Iglesia, 2021, p. 4)

Se establece como objetivo general del presente trabajo identificar operaciones de información en el conflicto Rusia – Ucrania en el periodo comprendido entre el año 2014 hasta febrero del año 2022, para poder relacionarlas con doctrinas extranjeras vigentes.

El alcance del presente trabajo tiene interés particular en el estudio de los acontecimientos en el conflicto Rusia - Ucrania en el nivel operacional, particularmente buscará determinar e identificar operaciones de información que se ejecutaron en dicho conflicto, desde la anexión de Crimea a Rusia hasta horas previas a que Vladimir Putin inicie con la operación especial sobre territorio ucraniano.

Respecto a las limitaciones que se pueden mencionar, principalmente, van a estar influenciadas por la constante evolución de la tecnología que va a incidir sobre las operaciones de información y su transformación ante estos cambios. También cabe destacar como limitación el estudio del conflicto hasta antes del inicio de las hostilidades por parte de Rusia el 24 de febrero del 2022.

Los aportes teóricos en el presente trabajo son mediante el análisis del conflicto, específicamente las operaciones de información, el análisis de la doctrina extranjera y determinar cómo se implementó esta en la ejecución de las operaciones de información. De esta forma abrir paso a futuros estudios para generar la doctrina ausente en nuestras fuerzas armadas, que es un vacío y afecta la defensa nacional.

De todo lo descripto deriva como hipótesis de la investigación si el conflicto entre Rusia y Ucrania demuestra el incremento de las operaciones de información ejecutadas por parte de los estados a nivel mundial en los conflictos actuales, lo cual se ha establecido como relevante y fundamental para obtener importantes ventajas en los procesos de toma decisiones.

Este trabajo de investigación será desarrollado bajo un enfoque cualitativo, siguiendo un diseño metodológico descriptivo.

Como técnica de recolección de datos se empleará el análisis bibliográfico, documental y de doctrina, se procederá con fuentes primarias como reglamentos vigentes de las Fuerzas Armadas Argentinas, tanto de carácter conjunto como específico, de Estados Unidos, de Brasil y de Chile, libros, revistas militares e informes específicos relacionadas con el tema en

cuestión. Con respecto a las fuentes secundarias, principalmente, se recurrirá a publicaciones del Instituto Español de Estudios Estratégicos, de la Fundación DIALNET y a Trabajos Finales Integradores de alumnos de la Escuela Superior de Guerra Conjunta.

Por último, el trabajo se desarrollará en dos capítulos; el primer capítulo tendrá por objeto analizar el escenario bélico entre Rusia y Ucrania para determinar operaciones de información que se ejecutaron. Como así también establecer las características generales de las Operaciones de Información. El segundo capítulo buscará contrastar la doctrina extranjera de Estados Unidos, Brasil y Chile con las operaciones de información determinadas en el capítulo uno.

Finalmente se extraerán conclusiones que permitan responder el problema planteado y satisfacer los objetivos ya descriptos. Aquellas conclusiones que respondan a estos lineamientos permitirán ratificar o rectificar la hipótesis de investigación planteada.

Capítulo I

Las Operaciones de Información en el Conflicto Rusia-Ucrania.

En el presente capítulo se abordan conceptos que permiten el análisis y comprensión de las operaciones de información del conflicto Rusia - Ucrania. Apunta principalmente a analizar el conflicto e identificar estas operaciones que fueron ejecutadas en el periodo desde el año 2014 a Febrero del año 2022.

De acuerdo a trabajos ya realizados por diferentes autores es importante recalcar que las Operaciones de Información son primordiales para llevar el éxito a las operaciones militares en la guerra, como a las actividades administrativas u operacionales en la paz. Las mismas tienen como Objetivo Principal contribuir a la maniobra operacional de los diferentes componentes de la fuerza, con la finalidad de controlar, dominar y mantener una supremacía en el empleo y explotación de la información. Esta información le permitirá al comandante llevar adelante una adecuada toma de decisiones, ya que la misma está constituida por datos esenciales o activos de importancia y en tiempo real, que ayudan a la conducción militar, y ofrecen una sustancial ventaja con respecto al oponente. (Bilibio, 2017, p. 5)

Cabe destacar que en la actualidad se transita en una “sociedad de la información” donde se mezcla el empleo de las fuerzas militares, tanto por sus medios desplegados o efectos que generan, como también por el impacto que tiene la información en la opinión pública a través de la cobertura del conflicto por parte de los medios de comunicación. (Soriano, 2010)

Es así que esta revolución de la información ha forzado a que evolucione la forma de lucha, como también ha logrado cambiar la forma de pensar de los individuos y su decisión a luchar por sus intereses. (Núñez, 2010)

1.1 Características Generales de las Operaciones de Información

Las operaciones de información están estrechamente vinculadas con otras operaciones y estas cruzan la campaña de lado a lado, siendo un elemento multiplicador de efectos sobre el oponente para disuadirlo, atacarlo o defender las posibles acciones que se lleven a cabo. (Bilibio, 2017, p. 7)

Los conflictos actuales están vinculados por una misma característica, que es el uso del conocimiento y la información para utilizarla como poder o contra el poder del adversario. Los estados o actores, generan las condiciones en el conflicto, a través de las operaciones de información, manejando e influyendo la percepción, a través de los medios de comunicación social, para poder confundir, influir, seducir a las fuerzas y a la sociedad del oponente. Influir en la percepción del oponente puede ser tan letal como el uso de las armas, ya que puede lograr el sometimiento sin la utilización de las mismas, y puede ser tan importante como la destrucción física.

Las Operaciones de Información en los Estados Unidos, son acciones que tienen la finalidad de manipular el sistema de decisión del oponente y se identifican como "Efectos No Letales" a los medios que se utilizan en este tipo de operaciones. En la publicación conjunta JP- 3-13, el Secretario de Defensa de los Estados Unidos define a las Operaciones de Información como "el empleo integral durante las operaciones militares de capacidades relacionadas con la información sincronizadas con las líneas de operaciones, para influir, dislocar, usurpar o corromper el sistema de decisión del adversario real o potencial y a la vez proteger el sistema de decisión propio." (Zarza 2016, p. 9)

La Organización del Tratado del Atlántico Norte (OTAN) define a una operación de información como: "una función militar para proporcionar asesoramiento y coordinación a las actividades militares de información para crear los efectos deseados en la voluntad, entendimiento y capacidad del adversario, potenciales adversarios y otros actores."

La definición anteriormente expuesta hace énfasis en el asesoramiento y coordinación de las actividades militares de información, esto lleva a tener en cuenta la importancia del asesoramiento y asistencia hacia el comandante en las operaciones, ya que si es el adecuado, el mismo estará en capacidad de tomar decisiones correctas para adelantarse al ciclo OODA del comandante enemigo y afectarlo, logrando una ventaja en las operaciones.

Las operaciones de información tienen como finalidad afectar principalmente la percepción cognitiva del entorno operacional, para que afecte al enemigo en el proceso de toma de decisiones y afecte su mente, de esta forma poder cambiar actitudes, hábitos, valores y lograr

la persuasión del enemigo, influyendo en su capacidad para explotar y proteger la información, sus sistemas de comando, comunicaciones, control, inteligencia e informática y logrando proteger los propios sistemas. (de Vergara & Trama , 2017)

Estas operaciones se encuentran dentro del ambiente de la información y se llevan a cabo para apoyar a cada componente en una operación totalmente integrada, buscando afectar las operaciones militares. Están compuestas por diferentes acciones que deben estar sincronizadas en el ambiente de la información y que puedan obtener y sostener el dominio del mismo. El comandante tiene la potestad de determinarlas en la oportunidad y lugar necesario para afectar capacidades operacionales, sistemas C3I2 (comando, control, comunicaciones, inteligencia e informática), opinión pública, información del oponente o en donde cree las condiciones para obtener la ventaja y lograr el objetivo. (Bilibio, 2017, p. 10)

Las capacidades militares que pueden abarcar dentro del ambiente de la información son las operaciones de guerra electrónica, operaciones de velo y engaño, operaciones psicológicas (comunicación social aplicativa al combate en la doctrina del Ejército Argentino, ROB 00-01), operaciones de Fuerzas Especiales, operaciones en la redes de información y operaciones de seguridad. (Bilibio, 2017, p. 11)

Estas capacidades que son operaciones, procedimientos o técnicas, según la doctrina española (Operaciones Conjuntas, Ejército Español, 2016,13A-11) pueden ser:

- Operaciones Psicológicas (*Psychological Operations* – PSYOPS).
- Presencia, Actitud y Perfil (*Presence Posture and Profile* – PPP).
- Seguridad de las Operaciones (*Operational Security* – OPSEC).
- Seguridad de la Información (*Information Security* – INFOSEC).
- Decepción- Engaño **(**MILDEC)
- Guerra Electrónica (EW).
- Destrucción Física.
- Operaciones de Redes Informáticas (*Computer Network Operations* – CON).
- Enlace, Conocimiento y contacto entre los Líderes Clave (KLE).
- Información Pública (PI)

Teniendo en cuenta las operaciones, procedimientos, técnicas, lugar de aplicación y finalidad de las mismas, es menester destacar que estas operaciones deben ser concebidas, planificadas y desarrolladas en el mas alto nivel del Teatro de Operaciones, el nivel operacional, con el fin de lograr el objetivo operacional de la campaña y de esa forma contribuir a los de la estrategia militar. Cabe destacar que la operacionalidad de las operaciones de

información se lleva a cabo en todos los niveles de la guerra, pero siempre conducidas desde el nivel operacional.

Sabiendo el nivel en el cual se conciben, se planifican y desarrollan estas operaciones, el comandante operacional debe tener en cuenta y considerar ciertos aspectos:

- Identificar objetivos de operaciones de información que faciliten el logro de la misión.
- Determinar la prioridad de los objetivos de las operaciones de información.
- Reorientar las operaciones de información ante nuevos acontecimientos militares.
- Asesorar al nivel estratégico y guiar al nivel táctico.
- Implementar medidas de respuesta ante una crisis. (Bilibio, 2017, p. 14)

El comandante al momento de concebir y luego planificar las operaciones de información deberá asignarles un efecto de acuerdo a lo que necesite afectar para poder cumplir con el objetivo de las mismas. La doctrina española, en el Reglamento Operaciones Conjuntas, Ejército Español, 2016,13A-28, establece los siguientes efectos: Informar: Dar propósito, objetivos y/o instrucciones; Advertir: Dar aviso de intenciones para evitar determinadas acciones del oponente; Persuadir: Predisponer hacia una acción o inacción; Desorganizar: Reducir una capacidad/eficacia evitando la sincronización de efectos; Aislar: Minimizar poder/influencia; Cooperar: Conseguir la cooperación; Promover: Reforzar positivamente una actitud o comportamiento deseado; Engañar: Lograr que una persona o grupo crea en algo que no es cierto; Adquirir información: Adquirir nuevos hechos, detalles, información general o específica; Negar: Negar información sobre las fuerzas propias, capacidades, situación, estado o intenciones al enemigo; Mejorar: Añadir a una situación ya positiva; Demostrar: Ofrecer información sobre capacidades o intenciones por medio de acciones convincentes; Disuadir: Desaconsejar, quitar de la cabeza determinada acción; Limitar: Reducir la eficacia enemiga reduciendo sus opciones o haciendo ver que alguna de sus tácticas de ser usada le causará efectos negativos no buscados por él; Influir: Causar que adversarios o neutrales se comporten de forma favorable a las fuerzas propias; Mitigar: Reducir o eliminar el impacto de una información falsa, un problema o una preocupación; Degradar: Usar medios letales o no letales para reducir: la eficacia o eficiencia del sistema comando y control del enemigo; la moral de una unidad o un público; el valor o relevancia de una unidad o público; la calidad de las acciones o decisiones enemigas.

El comandante es el que conduce y el que toma las decisiones en el teatro de operaciones, en las operaciones de información no es excluyente lo anteriormente dicho, pero deberá estar asesorado por un Jefe de operaciones de información que pertenece al estado mayor de su teatro. Este Jefe de operaciones de información tiene responsabilidades como las que se

nombran a continuación: Ser el oficial responsable de la integración de los efectos no letales para destruir o dislocar el flujo de información de las fuerzas enemigas; supervisar la protección de la información propia y del oponente; coordinar con otros miembros del estado mayor la integración de estas operaciones, coordinar con el oficial de Inteligencia las medidas de seguridad de contrainteligencia para llevar a cabo operaciones de información defensivas; integrar las operaciones de información dentro del "Proceso de Determinación de Objetivos" dentro de las operaciones de información ofensivas; coordinar las operaciones de velo y engaño, comunicación social aplicativa al combate, guerra electrónica para llevar a cabo las operaciones de información ofensivas; autorizar "Efectos No-letales" sobre blancos planeados; coordinar con el oficial de comunicaciones institucional" para publicar información como operaciones de información ofensivas. (Zarza 2016, p. 9)

Además de la finalidad, las capacidades y los efectos, las operaciones de información se tipifican como: operaciones ofensivas y defensivas.

Las Operaciones ofensivas son el ataque propiamente dicho en todos los niveles, sobre el personal, medios, medios e instalaciones informáticas, inteligencia y sobre la estructura de comando del oponente, en donde a través de los efectos anteriormente nombrados que contengan características ofensivas se busque lograr obtener el dominio y control del ambiente de información como también disminuir y degradar la estructura de información, comando y control, comunicaciones, informática e inteligencia del enemigo.

Las Operaciones defensivas: son aquellas operaciones que protegen los sistemas, de comando y control, medios, personas y medios de información e informática propios a través de medidas activas y pasivas, buscando disminuir los puntos débiles propios que el enemigo pueda afectar. (Bilibio, 2017, p. 16)

Para De Vergara y Trama en su publicación Operaciones Militares Cibernéticas, las Operaciones de Información en Ucrania, se constituyeron como las principales; y reflexiona sobre lo siguiente *"*el Ministerio de Defensa de Ucrania debió emigrar a otro país para poder dirigirse a sus fuerzas, ya que su acceso a los medios de comunicación ucranianos le estaba técnicamente vedado" (De Vergara Trama, 2017, p. 47). Este párrafo muestra la importancia de estas operaciones, que si son utilizadas de la manera correcta, la estrategia militar también se verá afectada y estará imposibilitada de llevar adelante las actividades básicas de la conducción. (Policante, 2019, p. 9)

1.2 Operaciones de Información en el Conflicto Rusia-Ucrania

Rusia tiene una larga tradición en el manejo de operaciones de información, especialmente en la desinformación y propaganda. Sus orígenes se encuentran en la revolución bolchevique, que desarrolló la propaganda leninista, y la Guerra Fría. En la década del 1950, el servicio de seguridad soviético (KGB), creó un departamento para la *desinformatsiya* que luego recibió el nombre de "medidas activas".

Es así que el uso de estas medidas activas no ha dejado de crecer y hoy en día es un pilar fundamental en el conflicto que lleva adelante Rusia en Ucrania, obteniendo resultados estratégicos.

Rusia se percata de la importancia de la información en la invasión a Georgia en el 2008. A partir de este momento, se genera la doctrina de la Guerra de Nueva Generación, que combina el despliegue de fuerzas militares como los componentes terrestres, marítimos y aéreos con la guerra por la información para afectar al oponente y a la opinión pública, en una dinámica de guerra híbrida. Por ende Rusia lleva el conflicto a que se desarrolle en un ámbito multidominio buscando explotarlos y dominarlos, especialmente en el ciberespacio y la información, utilizando todos los estamentos del estado, militares como no militares, tanto para hacer como para enfrentar la guerra híbrida.

Para llegar a un nivel adecuado de efectividad en las operaciones de información, Rusia despliega una estrategia de medios interagenciales que, abarca sus propios medios, financiados por ellos mismos, como también el uso intensivo de medios civiles como las redes sociales infiltrándose en los medios de comunicación social que no son afines, que toman la información suministrada informando la desinformación efectuada por Rusia. El canal más importante que inicio en el año 2005 es el canal Russia Today, y en el 2014 crean el canal Sputnik que llevaría la campaña informativa rusa con un plan de difusión de contenidos en 30 idiomas. (Jaspe Nieto, J. 2021, p.156)

En este periodo de la historia Rusa y sus relaciones internacionales, se ha aplicado la estrategia basada en la práctica de una guerra hibrida actualizada al contexto informativo y tecnológico contemporáneo. Para lograr sus objetivos, Moscú complementa sus actividades diplomáticas y militares con campañas de información multicanal y multilingüe, en su mayoría dirigidas a ejercer el control reflexivo diseñado por los artífices de la propaganda soviética. (Jaspe Nieto, J. 2021, p.162)

1.2.1 Anexión de Crimea a Rusia

En febrero de 2013, el General Valery Gerasimov, publicó un artículo titulado ¨El Valor de la Ciencia Está en la Previsión¨. Allí destaca que las reglas de guerra rusas han cambiado, y que los medios no militares tienen tanto o más poder que la fuerza de las armas para efectuar cambios en el escenario internacional. También aduce que las nuevas tecnologías han logrado reducir en las fuerzas tradicionales su capacidad de comando y control. Las acciones militares están dándole el paso a las acciones indirectas actuales, nuevas y subjetivamente más efectivas a través de las computadoras y la electrónica, esto se conoce como la Doctrina Gerasimov. (Círculo Militar, 2018, p. 151)

La oportunidad de la difusión y publicación de la Doctrina fue muy relevante ya que, poco tiempo después, Rusia invade Ucrania tanto con fuerzas, como con malware. La incursión digital en las redes, conjuntamente con un asalto militar físico, Rusia ya lo venia poniendo en práctica desde aproximadamente una década, ya sea en Estonia en 2007 y en Georgia en 2008. Los ataques se ejecutaron con finalidades que tenían efectos cibernéticos, efectos operacionales (con fuerzas), y combinación de efectos. (Círculo Militar, 2018, p. 151-152)

A inicios del 2014, la península de Crimea fue el foco de una de las peores crisis entre Rusia y Occidente desde la Guerra Fría, luego de que el presidente de Ucrania, Viktor Yanukóvich (prorruso), fuera derrocado tras protestas que tenían grandes tendencias europeístas. (BBC News Mundo, 2022)

El pueblo ucraniano estaba dividido entre los que querían una mayor relación con Rusia y los que estaban de acuerdo con una alianza con la Unión Europea (UE), es entonces que Moscú decidió intervenir. (BBC News Mundo, 2022)

Durante gran parte de febrero de ese año, Vladimir Putin había comenzado con una invasión silenciosa y secreta, llevando a cabo un trabajo de hormiga mandando de forma escalonada a miles de soldados adicionales a las bases que mantenía en Crimea, esto lo podía hacer ya que el Tratado de Partición de 1997 se mantenía vigente. También de la misma forma que envió militares enviaba ¨voluntarios¨ civiles. Este plan se completó con éxito y fue llamada la invasión suave. (BBC News Mundo, 2022)

Además del ingreso de militares y civiles Rusos, se estaba realizando un exhaustivo plan de desinformación a través de la propaganda en donde los líderes prorrusos aseguraban que necesitaban proteger a los habitantes de Crimea de los "extremistas" que habían tomado el poder en Kiev, derrocando al entonces presidente, y amenazaban el derecho del habla ruso en

la región. Cabe destacar que Yanukovic había enviado una carta al presidente de Rusia, pidiendo la intervención para restaurar el orden en Ucrania. (BBC News Mundo, 2022)

El primer indicio de que Crimea estaba siendo ocupada, se detectó el día viernes 28 de febrero, cuando Rusia instaló puestos de control en Armyansk y Chongar, los dos principales cruces de carreteras entre Ucrania continental y la península de Crimea. Estos puntos estaban controlados por hombres que llevaban uniformes muy variados, algunos vestidos como el ejército ucraniano, otros como la policía ucraniana, algunos con camuflaje sin insignia nacional, como también vestidos con ropa civil. (BBC News Mundo, 2022)

El 16 de marzo se realizó un referéndum (organizado por Rusia) en el que se llamaba a los integrantes de Crimea a votar para que esta sea una Republica Autónoma y se uniera a Rusia. Mientras tanto occidente hacia referencia a que lo que se estaba haciendo era totalmente ilegal. (BBC News Mundo, 2022)

Se realizó el acto de votación y el resultado de acuerdo a datos proporcionados por autoridades locales fue que el 95,5% de los votantes en Crimea apoyaban la opción de unirse a Rusia. Así mismo Putin ya había tomado la decisión y puesto en marcha la invasión.

Dos días después de la votación, el 18 de marzo, Vladimir Putin dio a conocer y oficializó la invasión y firmo un proyecto de ley en el que Crimea se incorporaba a Rusia, en donde pronuncio y aseguro que Crimea es ¨Tierra Santa Rusa¨.(BBC News Mundo, 2022)

La estrategia comunicativa que tuvo Rusia en este caso, y enmarcado dentro de las operaciones de información y que tiene una incidencia directa en Ucrania, es el discurso que se propagó, que se basó en la protección de la minoría étnica rusa y custodiar sus derechos. Dando como fundamento de esta protección a que en Ucrania se está procediendo a la censura de la lengua rusa. Esta supuesta situación desfavorable le dio la posibilidad de obtener un beneficio estratégico, que sin duda supo aprovechar. (Jaspe Nieto, J. 2021, p.158)

El objetivo de la anexión exitosa de Crimea por parte de Rusia en 2014 fue apoderarse del territorio sin recurrir a la fuerza militar abierta o convencional, una medida que ha alimentado el debate sobre la "estrategia híbrida" de Rusia. La anexión de Crimea se basó en gran medida en el despliegue de fuerzas especiales que operaron a través del comando de Fuerzas de Operaciones Especiales de Rusia recién creado. El despliegue de estas unidades de élite, combinado con la campaña de guerra de información y el despliegue de grupos con amplia simpatía por los objetivos rusos, o representantes, sentó las bases para una toma tradicional de Crimea sin derramamiento de sangre. (De Vergara Trama, 2017, p. 220)

1.2.2 Desinformación en la Guerra del Donbás

Como anteriormente se estableció, la desinformación es uno de los pilares de las operaciones de información que ejecuta Rusia. Esta desinformación está compuesta por noticias e información falsa que al estar concebida, planificada y desarrollada de una manera particular logra persuadir al público para que este se adhiera a ella. Cabe destacar que esta desinformación puede ser para ejecutar un ataque hacia un actor determinado mediante el procedimiento de la propaganda o para defenderse de los ataques que puedan afectar las capacidades mediante el procedimiento de la contrapropaganda.

Al hablar de desinformación uno de los casos más relevantes y trágico en el conflicto Rusia-Ucrania fue el derribo del vuelo comercial ¨MH17¨ de la aerolínea Malaysia Airlines. Este incidente, ocurrido en 2014 y según las averiguaciones y presiones internacionales se podría resaltar que los autores responsables del hecho, estarían en dirección a las tropas rusas.

Al poco tiempo del siniestro, y de acuerdo a las acusaciones y presiones de la comunidad internacional, el jefe de la Dirección General de Asuntos Político-Militares de las Fuerzas Armadas de Rusia, el Teniente General Andrei Kartapolov, realizó una rueda de prensa ante los medios para dar la versión oficial. El General, dio a conocer las pruebas circunstanciales que estaban destinadas a lavar la imagen y la duda que se había generado en la opinión pública sobre el hecho, llevando la responsabilidad indirectamente al ejército ucraniano del incidente. Sin mencionar específicamente la responsabilidad de Kiev, el Teniente General mostró imágenes satelitales del sistema de misiles antiaéreos Buk pertenecientes a las fuerzas armadas ucranianas en el área de vuelo de la aerolínea comercial Malaysia Airlines, lo que planteó la pregunta: "¿Por qué se desplego una cantidad tan grande de sistemas antiaéreos cerca de Donetsk?. (Jaspe Nieto, J. 2021, p.158)

Russia Today repitió las afirmaciones de Kartapolov en sus versiones en inglés y español al mismo tiempo que la conferencia de prensa. Ambos datos en sus sitios web estaban en los titulares de las noticias sobre la supuesta proximidad de un avión de combate Su-25 ucraniano a un Boeing 777 de Malaysia Airlines. Esta información agregaría otra incógnita para mitigar la responsabilidad rusa, creando confusión y volviendo a poner la duda sobre de Kiev. De esta manera también lograba hacer transparente el padrinazgo militar que tenía Rusia sobre las milicias rebeldes, estas milicias fueron y son una prioridad de la estrategia coordinada del alcance hacia occidente de los medios rusos. (Jaspe Nieto, J. 2021, p.158-159)

Días después, el 22 de julio de 201 , la edición en español de Russia Today prosiguió con la noticia de Kartapolov, lanzando en este contexto una serie de diez preguntas retóricas que

cuestionaban las acusaciones estadounidenses y daban a entender la actuación de las fuerzas ucranianas en el desarrollo de las acciones. Para ello, se centró en cuatro temas principales:

- El desvío del vuelo «MH17» de su ruta inicial.
- La actividad de los radares ucranianos.
- El despliegue de defensas antiaéreas ucranianas.
- La presencia del avión caza *Su-25* ucraniano. (Jaspe Nieto, J. 2021, p.159)

El desvío del vuelo ¨MH17¨ y la actividad de los radares ucranianos sugerían plenamente la participación de Ucrania al momento de dirigir de forma malintencionada la trayectoria del vuelo, y que esté al alcance de los misiles tierra-aire pertenecientes a ellos, lo cual demostraría la intensificación de la actividad de los radares militares ucranianos *Kupol-M1 9S18*. Al mismo tiempo, el despliegue de defensas antiaéreas ucranianas y la presencia del *Su-25* significaban intenciones y actividades hostiles dirigidas a la región de Donetsk. Finalmente, esa actitud ucraniana, según la justificación defendida por Rusia, habría llevado al derribo del avión, solo por razones relacionadas con el movimiento de tropas ucranianas. (Jaspe Nieto, J. 2021, p.159)

1.2.3 Operaciones Cibernéticas en Ucrania

1.2.3.1 Hackeo a la Red Eléctrica de Ucrania. En el invierno del año 2015, el día 23 de diciembre en la región de Ivano-Frankivsk, en el oeste de Ucrania, se produce un ataque cibernético al centro de control de Prykarpattyaoblenergo, que distribuye energía en la región. Dentro del centro de control, uno de los operadores detecto que en su computadora, el cursor de su mouse se deslizaba a través de la pantalla por su propia cuenta. Subsiguientemente se movió a los botones que controlaban los interruptores de la subestación en el área, hizo clic en una casilla que abrió los interruptores y apagó la subestación. Cuando esto sucedió, apareció un cuadro de diálogo que solicitaba confirmar la acción y el cursor confirmó haciendo un clic. Por lo tanto, la red eléctrica fue pirateada en gran parte de Ucrania y muchas personas y empresas perdieron electricidad esencial y valiosa durante la temporada invernal. (Wired, 2016)

Al intentar tomar el control del cursor, el mismo no respondió. Luego se mueve de un interruptor a otro, en ese momento la computadora deja de responder. El operador intentó desesperadamente volver a iniciar sesión, pero los atacantes habían cambiado la contraseña. La única acción que podía realizar era ver en la pantalla cómo los piratas abrían un interruptor tras otro, cerrando finalmente 30 subestaciones. Sin embargo, los atacantes no se detuvieron ahí. Continuaron atacando dos centros de distribución de energía simultáneamente, duplicando el número de subestaciones desconectadas y dejando a más de 230.000 personas a oscuras. Y

como si eso no fuera suficiente, cortaron las fuentes de alimentación de respaldo en dos de los tres centros de distribución, dejando a los propios operadores en completa oscuridad. (Wired, 2016)

Los piratas informáticos que atacaron los centros de energía ucranianos realizaron el primer ataque confirmado para derribar una red eléctrica, no eran oportunistas que simplemente atacaron las redes y lanzaron un ataque para poner a prueba sus habilidades, sino que fueron estrategas inteligentes y misteriosos que planificaron cuidadosamente su misión durante mucho tiempo, ejecutando los reconocimientos en primera instancia para examinar las redes y las credenciales del operador, y finalmente lanzar un ataque sincronizado. (Wired, 2016)

Los ataques comenzaron con una campaña de phishing dirigido a empleados y administradores de sistemas de varias empresas responsables de la distribución de energía en Ucrania. Hay 24 regiones, cada una dividida en 11 a 27 departamentos, y cada región es atendida por una empresa de distribución diferente. La campaña de phishing entregó correos electrónicos con documentos de Word maliciosos adjuntos a tres empleados. Cuando los empleados hicieron clic en el archivo adjunto, se les presentó una ventana emergente que les pedía que habilitaran macros para el documento. Al habilitarlo, un programa llamado BlackEnergy3 infectaba sus computadoras y dejaba abierta una puerta trasera para los piratas informáticos. Este método es notable porque la mayoría de las intrusiones explotaron fallas de codificación o vulnerabilidades en los programas de software. Sin embargo, en este caso, los atacantes aprovecharon una característica deliberada del programa Microsoft Word. La explotación de la funcionalidad de las macros es un método tradicional de la década de 1990 que fue revivido por los atacantes. (Wired, 2016)

En la intrusión inicial, los atacantes simplemente irrumpieron en la red corporativa. Sin embargo, necesitaban acceso a la red SCADA (Control de supervisión y adquisición de datos) que controla la red. Durante meses, realizaron un amplio reconocimiento, inspeccionaron y mapearon redes y obtuvieron acceso a los controladores de dominio de Windows que administran las cuentas de los usuarios de la red. Aquí recopilaron las credenciales de los empleados, algunas de las cuales eran para VPN (redes privadas virtuales). Una vez dentro de la red SCADA, se prepararon lentamente para el ataque. (Wired, 2016)

Tuvieron que reconfigurar el sistema de alimentación ininterrumpida (UPS) que proporcionaba energía de respaldo a dos centros de control. Crearon firmware malicioso para reemplazar el firmware original en los convertidores de serie a Ethernet en más de una docena de subestaciones. Retiraron los convertidores que evitaría que el operador envíe un comando

remoto para volver a cerrar el interruptor automático en caso de un corte de energía. (Wired, 2016)

Listos para atacar con el firmware malicioso, irrumpieron en la red SCADA a través de VPNs secuestradas y enviaron comandos para desactivar el sistema UPS ya reconfigurado. Luego comenzaron a abrir interruptores automáticos. Pero antes de eso, lanzaron un ataque telefónico de denegación de servicio en los centros de llamadas de los clientes, disuadiendo a los clientes de llamar para informar sobre las interrupciones. (Wired, 2016)

Cuando los atacantes abrieron los interruptores y desconectaron muchas subestaciones, también sobrescribieron el firmware en los convertidores de serie a Ethernet de la subestación, reemplazando el firmware original con firmware malicioso y provocando que los convertidores fueran inservibles. (Wired, 2016)

Después de hacer todo esto, usaron un malware llamado KillDisk para eliminar archivos de la estación del operador, dejándolos inoperables y provocando que las computadoras se bloqueen. (Wired, 2016)

La compañía publicó dos avisos en su sitio web, confirmando por primera vez que se había perdido el suministro eléctrico en ciertas áreas y asegurando que estaba trabajando para restaurarlo. Sin embargo, luego de que KillDisk finalizó su misión, la empresa emitió un segundo aviso, culpando a los piratas informáticos por la interrupción. (Wired, 2016)

Este fue un hackeo político de Rusia contra Ucrania. También cumplió el otro propósito de fastidiar a los clientes ucranianos y socavar la confianza en las empresas de energía y el gobierno. La inteligencia ucraniana dijo que Rusia estaba detrás del ataque cibernético en medio de las tensiones políticas entre los dos países. (Wired, 2016)

1.2.3.2 Ciberataque Masivo a Ucrania Ransomware Notpetya. En junio de 2017, Ucrania sufrió ataques masivos contra instituciones gubernamentales, comerciales, financieras y energéticas, provocando daños colaterales a empresas globales con oficinas en Ucrania como Maersk, FedEx y Merck. (CNET, 2018)

Fueron ejecutados por un ransomware llamado NotPetya. El ataque se produjo después de que se uniera el malware a MeDoc, el software de declaración de impuestos más popular de Ucrania. Desde allí se esparció a organizaciones multimillonarias con oficinas en Ucrania. El caso de Maersk ha resultado en una pérdida de ingresos de hasta 300 millones de dólares debido a los ataques. (CNET, 2018)

El malware no se diseñó para ser descifrado. En otras palabras, no había forma de que la víctima recuperara los datos una vez cifrados. Por lo tanto, es más exacto llamar a este ataque como más destructivo que un ransomware. (CNET, 2018)

El ataque, dirigido únicamente a Ucrania, llegó a más de 200.000 ordenadores en todo el mundo. Sin embargo, a diferencia del ransomware regular, NotPetya en realidad destruyó los datos, por lo que las víctimas no tenían forma de recuperar sus sistemas incluso después de pagar el rescate. (CNET, 2018)

El gobierno ucraniano encontró evidencias que vinculan el ataque con piratas informáticos rusos. Es así que llegaron a la conclusión de que era obra del ejército ruso y que este era parte del esfuerzo del Kremlin para desestabilizar Ucrania. (CNET, 2018)

1.2.3.3 Bots La Crisis del Agua en Ucrania en 2014. En el año 2014 después de la anexión de Crimea a Rusia, con un descontento y reclamo internacional, Rusia tuvo que tomar cartas en el asunto y es ahí en donde sigue con su plan de desinformación y propaganda. Es así que fueron publicadas varias historias por agencias de noticias rusas con la finalidad de engañar y confundir las audiencias seleccionadas como blanco, mediante la diseminación de desinformación a través de mentiras, y mala información procedente de información errónea. (Círculo Militar, 2018, p. 165)

La agencia de noticias ITAR-TASS mediante un esfuerzo coordinado a nivel estratégico disemina información de que le gobierno de Ucrania había dejado de trabajar en el canal norte que abastece de agua a Crimea desde el Rio Dnepr. Al mismo tiempo el canal de televisión internacional Russia Today (RT) anunciaba mediante la propagación de imágenes satelitales, que el gobierno ucraniano de manera arbitraria y adrede se empecinaba en lograr cortar el suministro de agua hacia Crimea, erigiendo una represa, y al mismo tiempo los científicos rusos no daban abasto tratando de encontrar agua para abastecer a Crimea. Al otro lado del mundo y tomando estas historias llenas de mentiras e información erróneas, el periódico ¨New York Times¨ hace uso de estas y publica que se estaba advirtiendo una insuficiencia de agua, y que las áreas agrícolas y ganaderas de Crimea habían comenzado con la sequía, que se estaba produciendo un grave problema de abastecimientos de alimentos y que los precios habían sufrido una suba sustancial. (Círculo Militar, 2018, p. 165)

Mientras tanto las fuerzas armadas rusas estaban empeñadas contra las fuerzas ucranianas en el este en operaciones de combate. El uso de Rusia de nuevas armas y métodos de combate no se limitó a capacidades no cinéticas. En el este de Ucrania, proyectiles termobáricos de racimo y de alto explosivo, destruyó de manera virtual y efectivamente a todo un batallón ucraniano en cuatro minutos. Lo que queda claro de la participación de Rusia en Ucrania es que Rusia utilizó y utiliza una gama de habilidades en formas nuevas e innovadoras para obtener una ventaja relativa en el campo de batalla. (Círculo Militar, 2018, p. 165)

Los bots prorrusos utilizaron Internet para formar un entorno de información en forma de cámaras de eco. El sesgo de confirmación perpetúa la información errónea, y cuando la información errónea rebota en la cámara de eco, deja un rastro en todos los lugares donde se encuentra. El bajo esfuerzo y costo, junto con el alto impacto de sembrar información a través de bots sociales, permite un impacto inmediato en las masas a corto y posiblemente a largo plazo. Estos bots difundieron noticias antioccidentales y prorrusas, dando al ejército ruso la oportunidad de lograr sus objetivos estratégicos antes de la posibilidad de una intervención occidental. Muchos bots copiaron el mismo artículo en otro sitio web o blog y luego simplemente lo tuitearon, pareciendo que el artículo se publicó por separado en una URL de sitio web diferente. O sea, los bots clonaban la desinformación, y creaban cámaras de eco y engañaban a la audiencia prevista sobre la operación militar en curso sobre Ucrania. (Círculo Militar, 2018, p. 166)

Los objetivos estratégicos de Rusia y la agresión resultante se trasladaron de Crimea a la propia Ucrania, pero la atención de los medios de comunicación del mundo no se desplazó en consecuencia. Si bien circuló información errónea sobre la crisis del agua, creada por los rusos, las fuerzas rusas operaron con relativa libertad dentro de las fronteras de Ucrania del este. (Círculo Militar, 2018, p. 167)

Tanto el hashtag ruso como el ucraniano, #Crimea, utilizaron el mismo algoritmo de filtrado y arrojaba resultados irregulares a diario. Temas como el fin del *alto el fuego y el avance de las tropas en el sureste de Ucrania* comenzaron a tener prioridad. La propaganda, el engaño, la desinformación y la capacidad de individuos y grupos para influir en diversas poblaciones a través de la tecnología social muestran la velocidad creciente de la interacción humana. La desinformación publicada en los medios de comunicación dejó a todos confundidos sobre lo que estaba pasando menos a los creadores. El control de esta ruta de comunicación en el dominio de la información se realizó mediante el uso implícito del control del discurso mediante botnets. (Círculo Militar, 2018, p. 167)

Capítulo II

Implementación Doctrinaria Extranjera

En el presente capitulo se identificará de acuerdo a las operaciones de información analizadas en los ejemplos históricos en el capítulo I, como los países de Estados Unidos, Brasil y Chile implementarían la doctrina para llevar adelante las capacidades desarrolladas en operaciones de información, específicamente en la desinformación y en las operaciones

cibernéticas u operaciones sobre redes informáticas que son las operaciones identificadas en los ejemplos históricos.

2.1 Doctrina de los Estados Unidos en las Operaciones de Información

La doctrina estadounidense establece que la información ha aumentado de forma exponencial en los últimos tiempos, y esto se debe al avance de la tecnología y con ello sus cuestiones positivas y negativas. Los individuos por más que se encuentren en cualquier lugar del mundo estarán en capacidad de comunicarse en tiempo real con otros sin quedar aislados. Pero las personas pueden pertenecer al bando amigo o enemigo, y esto comienza no solamente a ser algo positivo sino que también trae aparejado las amenazas, ya que con la información se esta en capacidad de influir, interrumpir, corromper o usurpar las capacidades de un adversario en el proceso de tomas de decisiones. (USA, 2014, p. I-1)

Las operaciones de información (OI) brindan a los comandantes americanos opciones flexibles y no letales. El efecto más importante depende de la capacidad específica principal que tenga el oponente. El objetivo estratégico de las OI es defenderse de las amenazas de posibles adversarios. (USA, 2006, p. 1-12)

Las capacidades militares de las operaciones de información incluyen la guerra electrónica, las operaciones de redes informáticas, las operaciones de apoyo de información militar, las operaciones de desinformación militar y la seguridad en las operaciones. Con la coordinación y el enfoque adecuados, estas capacidades pueden prevenir los conflictos armados. El propósito principal de estas operaciones a nivel estratégico es persuadir a los líderes o grupos de líderes clave para que se abstengan de ciertas acciones o, en su defecto, para que actúen en interés de los Estados Unidos. (Armistead, 2004, p. 16)

Las operaciones en redes informáticas según la Publicación Conjunta (Joint Publication) 3-13, Computer Network Operations, son capacidades básicas que están compuestas por tres subcomponentes, uno es el ataque contra redes informáticas, otro es la defensa de redes informáticas y por último la explotación de éstas. El enfoque de estas capacidades es producir un efecto disuasivo, pero la ofensiva o ataque a una red informática es el subcomponente que va a producir más efectos, logrando ser un auténtico ¨generador de efectos¨. El ataque debe usar las redes informáticas para negar, interrumpir o degradar computadoras, sistemas, redes informáticas o información resguardada por el oponente. Hoy en día la guerra evolucionó a depender cada vez más de los medios informáticos y así facilitar el comando y control de las operaciones. (USA, 2006, p. 1-12)

Los ataques a redes informáticas son armas masivas de interrupción contra blancos establecidos ya sean militares como no militares. (Williamson, J. 2002, p.9)

La desinformación militar es una capacidad básica y se enfoca en los objetivos más importantes que son los decisores del oponente, influyéndolos a sacar conclusiones erróneas a favor de los intereses propios. Como elemento disuasorio, crea sospechas, confusión y tal vez miedo entre los líderes del adversario, interrumpiendo o socavando el ciclo normal de toma de decisiones afectando el comando y control mientras intentan descifrar la desinformación. Los mensajes que contienen desinformación, datos erróneos o mentiras buscan generar desorden caos y conflictos internos, para que el oponente se desvíe de su curso de acción planificado y adopte posiciones más favorables a nuestros intereses. (USA, 1996, p. V-VI)

La propaganda que busca informar o desinformar, ejecuta la preparación del entorno de información en el territorio enemigo. La propaganda estratégica apoya a un oponente estratégico u operativo buscando repercutir en las opiniones, sentimientos, actitudes o comportamientos de las personas como posible objetivo de influir en las operaciones amigas. La operacional y táctica: la propaganda intenta incitar a la resistencia a las operaciones amigas dirigiéndose a las audiencias en el área de operaciones. La propaganda táctica también puede tratar de influir en las actitudes, sentimientos, motivos y razonamiento de los comandantes y miembros de las fuerzas amigas. (USA, 2003, p. 1-7)

En la doctrina norteamericana se identificaron las operaciones de información por parte de los rusos a Ucrania como la generación de desinformación militar y civil mediante propaganda a través de medios de información para lograr una invasión silenciosa, el hackeo a la red eléctrica de Ucrania, el hackeo de los sistemas informáticos enviando un ransomware masivo y el empleo de boots para generar desinformación luego de los reclamos y presión internacional luego de la invasión a Crimea.

2.2 Doctrina de la República Federativa del Brasil en las Operaciones de información

La evolución de la guerra es continua, el avance de la tecnología infunde en el área de la información junto con la sociedad, cambios más radicales y rápidos. Es así que las operaciones de información se convirtieron en una habilidad indispensable como herramientas integradoras de capacidades relacionadas con la información, que tienen diversos vectores que buscan informar a las audiencias amigas e influir las audiencias del oponente y neutrales en las operaciones de amplio espectro. Estas capacidades tienen como objetivo socavar la toma de decisiones de los potenciales adversarios y limitar su libertad de acción al intentar evitar,

prevenir o neutralizar los efectos de las acciones del oponente y proteger el proceso de toma de decisiones propio, en la dimensión de la información. (Ejército de Brasil, 2014, p. 2-7)

Las operaciones de información en Brasil contribuyen en buscar la superioridad de la información en el ambiente informacional, llevándolo a cabo con capacidades como: Comunicación Social, Operaciones de Apoyo a la Información, Guerra Electrónica, Guerra Cibernética e Inteligencia. (Ejército de Brasil, 2014, p. 3-1)

Para llevar adelante estas operaciones de información se deben aplicar principios que contribuyen al planeamiento y ejecución de estas operaciones. Cabe destacar que estas operaciones tienen un amplio espectro en el conflicto atravesando todas las operaciones dentro del teatro de operaciones. Los principios que se establecen son Unidad de comando, coordinación estrecha, inteligencia precisa, planeamiento centralizado al más alto nivel y ejecución descentralizada, planeamiento basado en efectos, participación y preparación temprana y luego de la ejecución análisis y seguimiento de los efectos logrados. (Ejército de Brasil, 2014, p. 3-2)

Las operaciones de información crean las condiciones del entorno operativo mediante un conjunto de actividades no militares que buscan identificar los riesgos potenciales y fuentes continuas de inestabilidad, reducción de incompatibilidades y eliminación de amenazas y detención de los acontecimientos que hacen que una crisis se agrave y finalice en conflicto. (Ejército de Brasil, 2014, p. 3-3)

Cuando se logra entender las características de estas operaciones se obtienen herramientas adecuadas para que los decisores de las Fuerzas tanto tácticos como operacionales y niveles superiores estén en capacidad de tomar adecuadamente decisiones y llevar adelante este tipo de operaciones, aplicando el Poder Nacional y militar. (Ejército de Brasil, 2014, p. 3-3)

La defensa y seguridad del ciberespacio de acuerdo a la revolución tecnológica, que en la actualidad se ha incrementado, es algo primordial que atender, ya que este es un dominio global que se encuentra dentro del ambiente informacional y por consecuente dentro del ambiente operacional. Esta dimensión informacional está compuesta por infraestructura crítica, datos y nuevas tecnologías, como el internet, los sistemas informáticos, procesadores y redes de comunicación. (Ejército de Brasil, 2014, p. 4-8)

Sobre este ciberespacio que se encuentran las infraestructuras, sistemas, etc se ejecutan las acciones cibernéticas. Estas acciones utilizan los recursos del ciberespacio y tienen como finalidad: proteger los activos de información, atacar y explotar las redes informáticas del adversario, afectando las condiciones normales de un área o región determinada, afectando gravemente el funcionamiento de estructuras estratégicas y servicios esenciales para la

población. Las acciones cibernéticas tienen como objetivo negar o manipular al oponente, mediante un medio de información (punto de acceso), un mensaje (mensaje encriptado), o una persona virtual (identidad “online” que facilita la comunicación, la toma de decisiones y/o la influencia desde una perspectiva cognitiva) (Ejército de Brasil, 2014, p. 4-8).

Las capacidades relacionadas con el área cibernética, cuando se destinan en apoyo de las operaciones de información, se enfocan en la integración de acciones ofensivas y defensivas realizadas dentro y/o a través del ciberespacio, en sintonía con los elementos del diseño operacional. (Ejército de Brasil, 2014, p. 4-8)

En la doctrina Brasilera se identifican los ejemplos históricos de las diferentes operaciones de información por parte de Rusia a Ucrania, como el sabotaje cibernético a la red eléctrica en Ucrania, el hackeo de los sistemas informáticos enviando un ransomware masivo a Ucrania, el empleo de bots para generar desinformación, mediante la guerra cibernética y la generación de desinformación mediante la propaganda a través de las operaciones Psicológicas, para persuadir al oponente y lograr una invasión silenciosa en Crimea.

2.3 Doctrina de la República de Chile en las Operaciones de Información

La cambiante situación en la que se encuentra el mundo y su seguridad, establece un cambio en la intensidad de la confrontación entre los estados potencias hacia relaciones complejas entre actores estatales y no estatales. La carrera por los recursos, las tensiones políticas, religiosas, sociales y la globalización incrementaron la incertidumbre. (Estado Mayor Conjunto de Chile, 2014, p. 15)

Esta cambiante situación se debe a la revolución tecnológica que se atraviesa, por lo tanto una revolución de información como el internet y la telefonía celular (desde donde se puede acceder a cualquier información), marca una época en donde las decisiones se determinan mediante computadoras. Es así que evolucionó y cambió el entorno de información que comprende a los estados o actores (líderes, individuos y organizaciones que toman decisiones) como la infraestructura que posibilita el uso de la información. La infraestructura de información cuenta con sistemas de información que recopilan, aplican y diseminan la información. En este entorno se mezclan las personas con los sistemas de información, y a través de ellos se decide, se observa y se actúa de acuerdo a la información que la atraviesa. (Estado Mayor Conjunto de Chile, 2014, p. 15)

Para lograr los objetivos de las operaciones de información en Chile, se puede emplear medios letales como no letales, pero cabe destacar que los medios no letales incrementaron en gran medida su empleo. Las operaciones de información le permiten al comandante elegir el

medio a emplear de acuerdo a la misión que deba cumplir. Al convivir en un ambiente dominado por la información estas operaciones han tomado mayor relevancia y aceptación, ya que la dependencia de estar informado y tener el conocimiento genera certidumbre. Es así que los medios de comunicación social los cuales difunden la información en tiempo real juegan un rol fundamental, ya que a través de ellos (internet, televisión, radios, etc) se puede explotar y manipular la información. Por ende la información cada vez juega un rol más relevante en los individuos como en las organizaciones. (Estado Mayor Conjunto de Chile, 2014, p. 15)

Los decisores van a tener efectividad en la toma de decisiones siempre y cuando tengan la voluntad de actuar, la comprensión y la capacidad para llevarlas adelante. Las actividades de información van a buscar influir y socavar en la voluntad del decisor adversario, pero van a proteger la voluntad del decisor propio, por otro lado van a buscar negar, degradar, manipular la información para influir en la comprensión del decisor, como también van a dar claridad para que el propio decisor tome las decisiones correctas, y por último van a afectar las capacidades del mando del adversario, pero van a fortalecer las propias. (Estado Mayor Conjunto de Chile, 2014, p. 18)

Las actividades de información, coordinadas a través de operaciones de información, son una parte integral del plan de campaña y están destinadas a influir en la voluntad y la comprensión de los responsables de la toma de decisiones y sus capacidades. Los efectos en el ambiente informacional contribuirán al logro de los objetivos de la campaña/operación. Estas operaciones de información involucran tres áreas de actividades interrelacionadas; Preservar y proteger la libertad de acción en el entorno de la información; Inducir, reforzar, influenciar, convencer y reafirmar percepciones, actitudes y comportamientos de audiencias; Defender la propaganda adversaria sus funciones y capacidades del mando que apoyan sus procesos de formación de opinión y de toma de decisiones. (Estado Mayor Conjunto de Chile, 2014, p. 21)

En el nivel operacional se desarrollan las actividades, procedimientos o técnicas de las operaciones de información, se definen los objetivos y efectos que se deben alcanzar. Debe existir un asesor de operaciones de información, que deberá coordinar con inteligencia, y la función mando y control, las que en forma integral deben proporcionar una capacidad militar decisiva al comandante de la fuerza. (Ejército de Chile, 2010, p. 21)

Los sistemas de telecomunicaciones e información (espacio electromagnético) y las operaciones de redes de sistemas informáticos (ciberespacio) son espacios críticos para el procesamiento de datos, la difusión y distribución de información, se realizan en plataformas técnicas y tecnológicas que deberán estar protegidas adecuadamente con operaciones de

seguridad en apoyo, ya que son el principal medio de comando y control de la fuerza. (Ejército de Chile, 2010, p.59)

En el planeamiento de las operaciones de información se deben analizar detalladamente las capacidades y redes informáticas propias y del oponente, y en especial los sistemas de telecomunicaciones e información, las operaciones en las redes de sistemas informáticas y las metodologías de toma de decisión del mando. Ya que un uso desproporcionado de estos sistemas, dejando de lado las adecuadas medidas de seguridad, generará vulnerabilidades y proporcionará al adversario una ventaja y un claro objetivo para su explotación y ataque. (Ejército de Chile, 2010, p. 59)

La protección y defensa de los sistemas que sustentan los ciclos de decisión, es una de las principales actividades a realizar por las operaciones de información en las redes informáticas. Esto se debe al avance y desarrollo de la tecnología informática que permite que los sistemas que intercambian información, desarrollen un papel clave para lograr procesos de toma de decisión eficaces. (Ejército de Chile, 2010, p. 60)

Las operaciones psicológicas como operación de información están dirigidas a una fuerza militar o a la población civil del oponente, para influir en su moral, actitudes, espíritu de lucha y comportamientos que afecten la percepción y opinión pública sobre la preparación militar de la fuerza adversaria y poder lograr los objetivos impuestos. Se deben usar medios de comunicación social, ya sean emisiones radiales, medios escritos y audiovisuales, televisión, Internet, también volantes, altavoces y otros medios de propaganda y de desinformación, para influir en las interpretaciones, actitudes, conductas y comportamientos individuales y grupales logrando la persuasión de la audiencia y así poder lograr los objetivos militares propios. (Ejército de Chile, 2010, p. 42)

En la doctrina chilena se puede identificar mediante las operaciones psicológicas como se implementaría la desinformación y propaganda que se ejecutaron en las operaciones de información de Rusia sobre Ucrania, como es el caso de la crisis del agua, el caso del vuelo comercial ¨MH17¨ de Malaisya Airlines y la invasión a Crimea. También se pueden identificar las operaciones cibernéticas, ya que desarrolla la importancia tanto del ataque, la defensa y explotación de las mismas. En esta doctrina se reflejaron los ejemplos históricos como el hackeo a la red eléctrica en Ucrania, el uso de boots para generar desinformación mediante una operación cibernética y el ciberataque masivo mediante un ransomware en Ucrania .

Conclusiones

A lo largo de la investigación se desarrollaron los contenidos siguiendo un hilo conductor y de acuerdo al objetivo general que fue establecido para este trabajo, el mismo es ¨identificar operaciones de información en el conflicto Rusia – Ucrania entre el año 2014 y el año 2022, para poder relacionarlas con doctrinas extranjeras vigentes¨ respondiendo al problema planteado ¿Cuáles son las Operaciones de Información en el conflicto Rusia – Ucrania encuadradas en el nivel operacional desde el año 2014 hasta el mes de febrero del 2022?

Los conflictos actuales, especialmente el de Rusia-Ucrania conlleva un gran desafío tanto para los actores como para el mundo, ya que genera incertidumbres, crisis en algunos casos y oportunidades en otros. Pero el mundo y los conflictos se encuentran atravesados por la globalización, el avance tecnológico, la personalidad de los líderes, por los comportamientos de las sociedades y especialmente por la información, que esta a través de la tecnología materializada en los medios de comunicación, traspasa el teatro de guerra y el mundo en cuestión de segundos, siendo una amenaza o una fortaleza.

Para Rusia en el conflicto contra Ucrania desde el año 2014 hasta fines de febrero del 2022, la utilización correcta de la información fue una fortaleza, ya que logro a través de sus capacidades ejecutar gran cantidad de operaciones de información, funciones, actividades y tareas, que ejecutadas por diferentes medios dependientes de un comando operacional contribuyeron con la campaña operando en el ambiente de la información. De esta forma pudo obtener objetivos estratégicos parciales y generar las condiciones necesarias para lanzar una invasión a gran escala sobre el este de Ucrania, denominada operación especial.

En estas operaciones que Rusia ejecutó en dicho periodo, se observó por un lado el cambio de enfoque de la guerra, en donde en un mundo dominado por la tecnología y la información, pero al mismo tiempo los actores dependiente de estas, Rusia buscó dominar el ambiente o dimensión informacional, que el mismo se encuentra dentro del ambiente operacional de una campaña, y a partir de allí generar efectos con medios flexibles y no letales que incidan en el comando, control, comunicaciones, inteligencia e informática del enemigo. Logrando así afectar, demorar e influir el proceso de toma decisiones de los decisores ucranianos, como también influir, acelerar, persuadir el procesos de toma de decisiones propios como los de sus aliados.

La ejecución de estas operaciones es de gran relevancia, ya que quien tenga la iniciativa de la ejecución, se va a adelantar al ciclo OODA (observar, orientar, decidir y actuar) del oponente, como se pudo ver en las acciones ejecutadas por Rusia, que tomaban por sorpresa a

la sociedad ucraniana y a sus decisores. Y se debe desestimar la actitud de esperar para responder ante este tipo de operaciones por parte del adversario, ya que eso generará vacíos y riesgos difíciles de contrarrestar. Por lo cual es imprescindible que la concepción y el planeamiento sea al más alto nivel y centralizado, para poder fijar de acuerdo a los objetivos estratégicos los propios objetivos operacionales, para luego poder ejecutar de manera descentralizada las operaciones en todos los niveles, antes, durante y después del conflicto. Estas operaciones afectan desde el nivel político pasando por la sociedad hasta el último soldado del teatro de operaciones.

Estas operaciones de información tanto en Ucrania como en el resto de los conflictos actuales, buscan legitimar las operaciones militares ante la opinión pública, esto se debe a que los medios de comunicación social participan activamente en la transmisión de información, para informar o influir, demostrando que estas operaciones conllevan la interagencialidad.

La doctrina analizada de los países de Estados Unidos, Brasil y Chile y en relación a las operaciones de información identificadas que fueron ejecutadas en el conflicto Rusia-Ucrania, cabe destacar que entre las tres doctrinas existe poca diferencia en su contenido. Esto se debe a que tanto la doctrina brasilera como la chilena son derivadas de la doctrina de Los Estados Unidos como de la Organización del Tratado del Atlántico Norte (OTAN) a la cual Estados Unidos pertenece como miembro principal. Esta doctrina se implementa y se modifica de acuerdo a los cambios que suceden con gran velocidad en los conflictos actuales, ya que estos actores participan activamente en ellos.

Esta doctrina tiene procedimientos y finalidades similares, y buscan lograr efectos que contribuyan al desarrollo de las propias operaciones, como también disminuyendo afectando o influyendo el efecto de las operaciones del enemigo, y en todos los casos explotar debilidades para lograr los objetivos.

Cabe destacar que la doctrina también va a estar cruzada por la idiosincrasia de cada país, lo cual va a provocar que se ejecuten o se desarrollen las operaciones de forma diferente.

En esta doctrina extranjera se logró identificar las operaciones de información y la implementación de la misma. En donde a través de la desinformación militar, la propaganda y operaciones sobre redes informáticas se logra generar los efectos necesarios para obtener los objetivos que Rusia obtuvo sobre Ucrania con las operaciones de información.

Teniendo en cuenta esta doctrina extranjera que se analizó, y a causa de que existe un vacío en la doctrina de las Fuerzas Armadas Argentinas, resulta imperioso la elaboración de la misma para implementarla en forma integral junto con las operaciones de combate. Así mismo se establece y contempla en la doctrina argentina la Guerra de la Información, pero no define las

operaciones de información a desarrollar, como tampoco las organizaciones que tienen la capacidad para ejecutar estas operaciones, en resumen las Fuerzas Armadas Argentinas no cuentan con las capacidades para la ejecución de operaciones de información.

La ejecución de estas operaciones da una ventaja cuantiosa a quien las ejecuta porque le da la posibilidad de poder crear las condiciones deseadas para obtener los objetivos quizás sin ejecutar un solo disparo. Con estas operaciones no se va a ganar la batalla, pero si van a contribuir a la misma.

Quien no ejecute operaciones de información, se encuentra en total desventaja frente a quien si las realiza, ya que estas van a inclinar la balanza de manera considerable. La influencia de estas operaciones en tiempos de crisis o guerra puede generar que un ejército pierda su voluntad de lucha, siendo persuadido a abandonarla.

Es por eso que resulta imprescindible, para estar a la altura de la situación y ser Fuerzas Armadas profesionales, la creación de la doctrina necesaria para llevar a delante estas operaciones y tener la preparación adecuada, y así poder afrontar los desafíos de las guerras que se viven, especialmente en los desafíos informáticos que impone el mundo globalizado. Por ende, si no se está preparado para afrontarla, se comienza el conflicto con ciertas posibilidades de que se puede fracasar.

Lo más importante para las Fuerzas Armadas, es la preparación para la guerra y así poder defender sus intereses. Esta preparación se logra mediante el estudio de la doctrina, la experiencia de guerra que pueda tener, y a través de la adaptación de la doctrina a la práctica y la adaptación de la doctrina a los continuos y rápidos cambios que se producen en el mundo.

Finalizando y luego de haber analizado el conflicto de Rusia-Ucrania e identificado operaciones de información ejecutadas y habiendo analizado doctrina extranjera con respecto a estas operaciones se puede concluir que: las operaciones de información de acuerdo a la revolución tecnológica e informacional en la cual se encuentra el mundo, han tomado gran relevancia, por lo cual se incrementó la ejecución de las mismas, siendo estas una capacidad fundamental en los conflictos actuales para lograr afectar al enemigo y obtener ventajas en los procesos de toma de decisiones.

Bibliografía

Armistead, L. (2004) *Information Operations: Warfare and the hard Reality of Soft power*. Washington.

BBC News Mundo. (26 de Febrero de 2022) *Rusia y Ucrania: Que paso en Crimea y porque ahora importa*. Recuperado el 24 de septiembre del 2022 de https://bbc.com/mundo/noticias-internacional-60500020.

Bilibio, R. M. (2017). *La importancia de la aplicación de las operaciones de información en un ambiente operacional. CABA.*

Campos, G. (2021). Curso de Oficial de Estado Mayor. Materia: *Inteligencia Estratégica*. Buenos Aires, Argentina: Escuela Superior de Guerra del Ejército Argentino.

Círculo Militar. (2018) *Percepciones son realidad: Estudio de casos históricos de operaciones de información en operaciones de combate a gran escala*. CABA.

Colom, P. G. (2018). *La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo*. Madrid, España: Revista del Ejército de España Nro933 -.

CNET. (15 de Febrero de 2018) *Russia´s Notpetya the most destructive cyberattack ever*. Recuperado el 24 de septiembre del 2022 de https://cnet.com/news/privacy/uk-said-russia-is-behind-destructive-2017-ciberattack-in-ukraine/.

de Vergara , E., & Trama , G. A. (2017). *Operaciones Militares Cibernéticas - Planeamiento y Ejecución en el Nivel Operacional.* CABA: Visión Conjunta, 125. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres* (ROB - 00 - 01). Buenos Aires: Departamento Doctrina.

Ejército de Brasil. (2014). *Operacoes de Informacao* (EB20-MC-10.213). Ministerio da Defensa.

Ejército de Chile. (2010). *Operaciones de Información*. (RDO-20909) Santiago de Chile: División Doctrina.

Ejército de Estados Unidos, FM 3-13 (2003) *Information Operations*. Washington.

Erickson, J. V. (2022). *Clausewitz sobre la disuasión de las actividades malignas rusas en el ciberespacio.* Kansas: Military Review.

Escuela Superior de las Fuerzas Armadas Españolas (2016). *Operaciones Conjuntas.* Departamento Operaciones.

Estado Mayor Conjunto de Chile, (2014) *Operaciones de informacion conjuntas*. (DNC 3-7). Ministerio de Defensa Nacional.

Estado Mayor Conjunto de Estados Unidos, JP 3-13 (2006) *Information Operations.* Washington.

Estado Mayor Conjunto de Estados Unidos, JP 3-13 (2014) *Joint Operation* 3-13. Washington.

Estado Mayor Conjunto de Estados Unidos, JP 3-58 (1996) *Joint doctrine for military deception*. Washington.

Ferrari, Vigón, Gaggero. (2001). *La Revolución de Asuntos Militares y la Guerra de la Información.* Buenos Aires, Argentina: Escuela Superior de Guerra.

Jaspe Nieto, J. (2021) *Las operaciones de información Rusas en el conflicto del este de Ucrania*. Revista Comunicación y Hombre, 17. Madrid

Keller, Cuello, Tabbia. (11 de Agosto de 2004). Trabajo Final de Licenciatura en Estrategia y Organización. *Los Procesos de Comunicación y la Anticipación de Crisis. Gestión de Estrategias Comunicacionales en la Organización ante casos de alta resonancia pública y su vinculación con el Liderazgo.* Buenos Aires: Escuela Superior de Guerra.

Leimete, M. G. (2019). *Ucrania, estrategia y geopolítica bajo la influencia de la OTAN, la UE y Rusia*. Buenos Aires.

Márquez de la Rubia, F. (2019). *Ucrania: algo más que elecciones*. Documento de Análisis IEEE 04/2019. Madrid: Instituto de Estudios Estratégicos de España.

Núñez, N. M. (2010). *Apoyo Público a Operaciones Militares: Factores Clave.* Cuaderno de Estrategia Nro 148 Madrid: Instituto Estudios Estratégicos de España.

Pardo de Satanyana, J. (2021). *¿Por qué a Rusia le interesa tanto Ucrania?* Documento de Análisis IEEE 25/2021. Madrid: Instituto de Asunto Estratégicos de España.

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

Quiñones de la Iglesia, F. J. (2021). *Desinformación y subversión (2.0): las técnicas de la Guerra Fría reaparecen en el dominio informativo del siglo XXI*. Documento Marco IEEE 12/2021. Madrid: Instituto de Estudios Estratégicos de España.

Sánchez Herraes, P. (2014). *La nueva guerra híbrida: un somero análisis estratégico.* Documento de Análisis IEEE 54/2014. Madrid: Instituto de Estudios Estratégicos de España.

Sánchez Herraes, P. (2015). *Crisis de Ucrania: Nueva guerra fría o solución cubana?* Documento de Análisis IEEE 37/2015. Madrid: Instituto de Estudios Estratégicos de España.

Sánchez Herraes, P. (2016). *Rusia: ¿el retorno al paradigma del empleo de la fuerza militar?* Documento de Análisis IEEE 32/2016. Madrid: Instituto de Estudios Estratégicos de España.

Spretz, N. (2018). *Las operaciones de información de nivel operacional y su influencia en el ambiente informacional.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Torres Soriano, M. R. (2011). *"Guerras youtube. El impacto de las nuevas tecnologías de la información en el tratamiento mediático de los conflictos armados*." Cuadernos de Estrategia Nro 148.

USA Joint Chiefs of Staff. (2016). *Information Operations* (FM 3-16). US Military.

Williamson, J. (2002) *Information Operations: Computer Network Attack in the 21st Century*. Pensilvania

Wired. (3 de Marzo de 2016) *Inside the cunning unprocedented hack of Ukraine´s Power Grid*. Recuperado el 24 septiembre del 2022 de https://wired.com/2016/03/inside-cunning-unprocedented-hack-ukraines-power-grid/

Zarza, L. (2016). *Estrategia Militar y su transfiguración en la era de la información*. CABA: Visión Conjunta, 15. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.