TRABAJO FINAL INTEGRADOR

TEMA:

El uso de la ciberguerra en las guerras en curso

TÍTULO:

Las operaciones de ciberguerra y su contribución al logro de los objetivos del nivel operacional: caso de estudio el accionar de Rusia contra Ucrania

Belletti, Federico

Año 2021

RESUMEN

Con la evolución de la tecnología conforme a los avances de los Estados y la explotación y usufructo del quinto dominio, el ciberespacio, se abre una nueva era en el desarrollo de los conflictos armados. Atrás quedan los desafíos por imponer la voluntad o lograr la superioridad aérea, marítima, terrestre o espacial. El advenimiento de este nuevo dominio obliga a los Estados a estar preparados porque la agresión, al igual que los ataques, son producidos de manera silenciosa, sin necesidad de efectuar una gran movilización de las fuerzas armadas.

El presente trabajo describe las causas que han dado origen al conflicto entre la Federación de Rusia y Ucrania, país perteneciente a la ex Unión Soviética, en la cual el país ruso aún posee claros intereses y ha efectuado operaciones de ciberguerra y de información para alcanzar sus objetivos propuestos.

En tal sentido la Rusia ha creado una revolución a la hora de llevar adelante sus conflictos con otros Estados, lo cual ha generado una gran preocupación en los países de occidente. El empleo de herramientas convencionales con otras no convencionales, constituyen la manera de disponer sus enfrentamientos contra estos, donde la superioridad de la información es esencial para imponerse al adversario.

El conflicto con Ucrania es un claro ejemplo de lo expresado aquí donde operaciones cibernéticas y de información alteran o modifican la situación reinante en un país, lo que motiva a preguntar cómo contribuyen las operaciones de ciberguerra desarrolladas por la Federación de Rusia en el conflicto con Ucrania al logro de los objetivos operacionales.

Finalmente, el objetivo de la investigación es determinar la contribución de las operaciones de ciberguerra al logro de los objetivos establecidos por el nivel operacional en el conflicto ruso-ucraniano.

PALABRAS CLAVE

Ciberespacio– Ciberguerra – Información – Rusia – Ucrania

ÍNDICE

GLOSARIO[1]

Botnet: es un conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc.

Hacker: Persona que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política.

Hacktivista: Ciberdelincuente que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política.

Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.

Phishing: Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

Spear phishing: Modalidad de phishing dirigido contra un usuario u organización en concreto en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir información confidencial.

[1] Extraído del Instituto Nacional de Ciberseguridad, *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario*, Gobierno de España, Secretario de Estado de digitalización e inteligencia artificial.

INTRODUCCIÓN

La ciberguerra tiene su origen en la década de los noventa cuando se comenzaron a explotar los amplios recursos que brindaba la herramienta internet. Durante el transcurso de la primera década del siglo XXI, a través del empleo y usufructo del ciberespacio, se comenzaron a efectuar operaciones para vulnerar, modificar y distorsionar información sensible y clasificada de los Estados.

En este contexto, la Federación de Rusia ha sido una de las principales potencias del mundo que ha efectuado ataques cibernéticos contra países sobre los cuales sus intereses han sido manifiestos, como ser Estonia en el año 2007 y Georgia en el año 2008. En la actualidad el mencionado Estado se encuentra en un enfrentamiento con Ucrania país que formo parte de la antigua Unión Soviética hasta la disolución de esta en 1991. En ella Rusia posee intereses, dado la manifiesta decisión del pueblo ucraniano de querer ser parte de la Unión Europea, a excepción de los pueblos o regiones que continúan siendo pro rusas.

En este nuevo conflicto, el gobierno ruso ha decidido emplear nuevamente herramientas que constituyen parte de las guerras híbridas como lo son las operaciones de ciberguerra. La explotación de este nuevo dominio modifica el ambiente operacional tradicional, y por ende es necesario conocer cómo es su accionar a la luz del nivel operacional. El propósito de la presente investigación es determinar cómo han sido empleadas las operaciones cibernéticas por parte de Rusia en contra de Ucrania, a los fines de poder determinar cómo las operaciones de ciberguerra y de información influyen para contribuir con el logro de los objetivos establecidos por el Nivel Operacional.

Las guerras han ido evolucionando conforme al progreso de las sociedades y al desarrollo tecnológico que esto ha traído aparejado. En las denominadas guerras de cuarta generación o asimétricas, el autor que le diera existencia a tal nombre, William S. Lind, considera que se desarrollan con características totalmente distintas a las tres generaciones anteriores. En estos conflictos la tecnología tiene un papel trascendental para su desarrollo, y la distinción del enemigo en el campo de batalla es difícil de poder identificar en virtud de los actores militares y civiles que participan en este (Ayerve, 2019).

Las amenazas que se presentan son asimétricas y tienen la particularidad de estar constituidas por operaciones convencionales y no convencionales. Los elementos del

combate convencional lo constituyen las fuerzas armadas de cada nación en los enfrentamientos entre estos, mientras que en las operaciones no convencionales se encuentran fuerzas especiales de los Estados, células terroristas, como también organizaciones no gubernamentales entre otras (Trama, Guerrero, & de Vergara, 2019).

Esto significa que la amenaza que se presenta en los conflictos actuales es de característica híbrida, donde se enfrentan no solo fuerzas armadas de distintos países, sino que también se presentan otros actores y acciones –diplomáticas, legales, sociales, económicas–con los mismos objetivos que los ejércitos tradicionales. Estos diferentes tipos de intérpretes persiguen cómo propósito alcanzar lo establecido por el poder político, en otras palabras, el estado final deseado.

En esta clase de conflictos, se comienza a explotar el quinto dominio, o sea, el ciberespacio y con este también surgen nuevos tipos de amenazas dentro del escenario bélico, produciendo una hibridación de las contiendas (Ayerve, 2019). Bajo este nuevo contexto es que se comienzan a usufructuar las bondades que brinda este nuevo escenario, donde son muchos los Estados que se enfocan en él, con la finalidad de estar preparados para las exigencias que demandan los enfrentamientos modernos. De esta manera, mediante la explotación del ciberespacio, comienzan a desarrollarse las primeras agresiones cibernéticas.

Estos ataques informáticos se infiltran en distintos sistemas con el propósito de recabar información, distorsionarla, o denegar accesos a los sistemas de diferentes usuarios entre otras finalidades. En tal sentido, son cada vez más los Estados que se encuentran desarrollando capacidades informáticas con la necesidad de actuar en un ambiente operacional cada vez más complejo. Por tal razón, se encuentran creando ejércitos de ciber soldados de manera de poder hacer frente a esta nueva amenaza y lograr actuar defensivamente en caso de ser pasible de recibir algún tipo de ataque (Medero, 2010).

En cuanto al significado de qué es la ciberguerra, se puede decir que son numerosas las definiciones existentes de este tipo operación. En la República Argentina, el Decreto 457/2021 –actualización de la Directiva de Política de Defensa Nacional– en su Anexo entiende la evolución del ciberespacio como un ambiente para el desarrollo de operaciones militares que atraviesa a los espacios tradicionales, y define a las operaciones de ciberguerra como a aquellas que:

> (…) poseen su origen en el ámbito virtual de los sistemas informáticos y las redes de comunicación, también pueden impactar sobre el mundo físico. Esto es tangible en los recaudos cada vez más expandidos en ámbitos tan variados como el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, las comunicaciones militares y la capacidad de mando y control, entre otros (Decreto 457/2021)

Mientras, otra definición es la de la Organización de las Naciones Unidas que establece lo siguiente:

> (…) una guerra cibernética significa el uso de computadoras o medios digitales por un gobierno o con el conocimiento explicito o la aprobación de ese gobierno contra otros estados, o propiedad privada dentro de otro Estado incluyendo: el acceso intencional, interceptación de datos o daños a la infraestructura digital y a la infraestructura controlada digitalmente; y la producción y distribución de dispositivos que pueden usarse para subvertir la actividad interna. (Trama & de Vergara, 2017, pág. 37)

Como se puede observar en las definiciones expuestas existe un común denominador en todas ellas y es el uso de medios virtuales, para ocasionar o infligir daño a otro, en infraestructuras físicas como digitales.

La ciberguerra tal como lo enunciase Trama difiere del conflicto armado convencional dado que a diferencia de aquella los oponentes pueden librarla de manera rápida, económica, anónima y devastadora, desde cualquier parte del planeta (Trama G. A., 2017). El objetivo que se persigue con la ciberguerra es el uso del ciberespacio como parte del ambiente operacional, donde mediante el uso de armas no cinéticas, se busca destruir, anular o neutralizar, las infraestructuras críticas de una nación, como así también el comando y control de las fuerzas armadas del enemigo. Otro tipo de efecto que se busca alcanzar es afectar las instituciones de los Estados, la moral y seguridad de la población y a la vez proteger las propias capacidades.

Cuando un Estado emplea la ciberguerra a los fines de producir efectos contra su enemigo o protegerse de agresiones cibernéticas por parte de este, lo efectúa realizando operaciones cibernéticas de carácter ofensivas y defensivas respectivamente mediante el uso de las capacidades del ciberespacio. Las ciberoperaciones, “son aquellas operaciones que son ejecutadas para interrumpir, negar, degradar o destruir la información existente en las computadoras y redes de computadoras, o las computadoras y redes propiamente dichas” (Trama & de Vergara, 2017, pág. 88).

Otro tipo de acciones que se desarrollan con el apoyo de las capacidades del quinto dominio, son las operaciones de información. Al respecto Trama y de Vergara (2017) establecen que:

> (…) cuando las capacidades cibernéticas se emplean en apoyo de las operaciones de información, el efecto que se pretende lograr es negar o manipular la toma de decisiones del adversario o de un potencial adversario, impactando sobre un medio de información (como un punto de acceso inalámbrico en la dimensión física), el mensaje propiamente dicho (un mensaje cifrado en la dimensión de la información), o a una cyber-persona (una identidad en línea que facilita la comunicación, toma de decisiones y la influencia de las audiencias en la dimensión cognitiva) (Trama & de Vergara, 2017, pág. 236).

Una de las grandes potencias mundiales que se ha perfeccionado en el empleo de este nuevo tipo de ataque no cinético es la Federación de Rusia. Se habla que la primera ciberguerra aconteció en los ataques perpetrados por el mencionado país a Estonia en el año 2007, e inclusive volvería a emplearla al año siguiente contra Georgia y en el año 2013 contra Ucrania.

En el conflicto con Georgia en 2008, las ciberoperaciones tuvieron un papel trascendental, seguidas de las acciones ejecutadas por las fuerzas especiales. En este acontecimiento las fuerzas convencionales fueron consideradas y empleadas en un segundo plano (Trama & de Vergara, 2017).

A finales de 2013, Ucrania vivió una fuerte crisis interna a raíz de la división de su población entre quienes apoyaban la decisión de formar parte de una asociación con la Unión Europea y los que la rechazaban por su identificación pro-rusa. Como consecuencia de esto, la Federación de Rusia se encuentra en conflicto con Ucrania, donde en el año 2014 el Estado ruso anexó la península de Crimea como parte de su territorio, y combatientes separatistas apoyados por Moscú comenzaron un enfrentamiento armado en las óblast de Donetsk y Lugansk, perteneciente a la región de Donbás.

Durante el desarrollo de este conflicto, los ataques cibernéticos efectuados por Rusia han causado, entre otros, daños temporales sobre la infraestructura critica del país ucraniano. El Estado ruso ve el empleo de la ciberguerra de una manera muy diferente a como lo ven los países de la OTAN, en función de cómo la definen y utilizan, donde herramientas no militares son tan eficientes para alcanzar los efectos deseados como las militares.

En la actualidad, la Federación de Rusia emplea lo que se conoce en el mundo occidental como Doctrina Gerasimov. Este nombre responde al nombre del General Valery Gerasimov, quien señalo el carácter cambiante de las guerras y la evolución del uso coordinado de medidas militares y no militares. Este sugiere que las medidas no

militares prevalezcan sobre el poder militar, el cual se empleará solo cuando no se puedan lograr los objetivos establecidos por los métodos no militares (Bilyana & Cheravitch, 2020).

Otro concepto de la doctrina Gerasimov es que "el uso de Internet ha revolucionado el espacio informativo y abrió infinitas posibilidades para degradar tanto la capacidad militar del enemigo como erosionar el liderazgo político y la opinión pública del adversario" (Makotczenko, 2019, pág. 21).

En tal sentido, es importante destacar que las fuerzas armadas rusas no emplean el término ciberguerra. Este concepto es encuadrado dentro de un marco más amplio que es el de la guerra de la información, el cual incluye operaciones de redes informáticas, guerra electrónica, operaciones psicológicas y operaciones de información (Connell & Vloger, 2017).

El concepto de guerra de la información, que incluye a la ciberguerra, encaja a la perfección con el carácter cambiante de la guerra que establece el general ruso, ya que estas se efectúan en un ambiente donde no existen las fronteras que limitan entre los Estados. Las operaciones que efectúa brindan la posibilidad de influir de manera encubierta no solo sobre las infraestructuras críticas de la información, sino también sobre la población de un país, lo cual afecta la seguridad nacional de los Estados (Bilyana & Cheravitch, 2020).

Las fuerzas armadas rusas contemplan que las capacidades cibernéticas ofensivas son idóneas para las guerras actuales por su versatilidad, eficacia y bajo costo; ya que permite que las operaciones cibernéticas puedan hacer desaparecer los límites entre la guerra y la paz, dado a que se puede ocasionar agresiones a un enemigo en tiempo de paz sin haberse declarado la guerra como un acto legal. Sin embargo, lo más importante para Rusia es que las capacidades cibernéticas ofensivas pueden ser consideradas como acciones asimétricas que posibilitan que un país con tecnología y una economía más débil puede neutralizar a un adversario considerado más fuerte (Bilyana & Cheravitch, 2020).

De esta manera, con la explotación del denominado quinto dominio, el ambiente operacional en un enfrentamiento bélico cambia radicalmente, esto responde a que ahora las amenazas no solo son ejecutadas dentro del teatro de operaciones, sino que pueden ser llevadas adelante desde cualquier lugar del mundo. También se modifica el efecto que se busca alcanzar con su implementación, ya que mediante el desarrollo de operaciones

cibernéticas y operaciones de información se persigue producir caos y confusión en las fuerzas militares, población y en las autoridades gubernamentales.

En función de los descripto precedentemente, donde en los conflictos actuales se emplean fuerzas convencionales con otras herramientas no convencionales, es deseable considerar como las operaciones de ciberguerra son cada vez más importante en el desarrollo de estos, donde países como la Federación de Rusia hace uso de sus bondades, razón por lo cual se debe analizar como las mismas influyen para poder alcanzar los objetivos previstos durante el desarrollo de una contienda. Por tal motivo es que surge el interrogante que origina el desarrollo del presente trabajo final integrador: ¿Cómo contribuyen las operaciones de ciberguerra desarrolladas por la Federación de Rusia en el conflicto con Ucrania al logro de los objetivos operacionales?

En la presente investigación se realizará un estudio de las operaciones cibernéticas y de información llevadas adelante por la Federación de Rusia contra Ucrania en el conflicto que tuvo sus orígenes a finales del año 2013. Para ello, en primera medida será necesario identificar cuáles son las causas que desencadenaron en el enfrentamiento entre ambos países, como así también el porqué de la importancia que reviste la península de Crimea para el gobierno ruso. Asimismo, se analizará la incidencia que tienen las operaciones de ciberguerra en el nivel operacional.

El trabajo se limitará a las operaciones de ciberguerra que fueron efectuadas durante el desarrollo del conflicto ruso-ucraniano. Mientras que la finalidad que se persigue con la elaboración del presente trabajo de investigación es poder determinar las contribuciones que las operaciones de ciberguerra efectuadas en el conflicto de Rusia con Ucrania, pueden brindar para que los objetivos establecidos en el nivel operacional puedan ser alcanzados.

Con este estudio de caso se busca aportar al área del arte operacional, donde mediante la descripción y el análisis de las operaciones de ciberguerra efectuadas durante el conflicto entre los Estados de la Federación de Rusia y de Ucrania se pretende establecer cómo inciden en el nivel operacional. También posibilitará comprender cómo en las guerras del siglo XXI existe una marcada participación y empleo de las amenazas híbridas, como lo son la guerra cibernética y las operaciones de información, en las cuáles se emplean operaciones de características no cinéticas para alcanzar el estado final deseado estipulado por en nivel estratégico nacional.

Asimismo, este trabajo buscará determinar cuáles son las contribuciones que el empleo de las operaciones de ciberguerra puede brindar al nivel operacional, para que este alcance los objetivos establecidos, mediante la ejecución de operaciones cibernéticas y operaciones de información.

Para poder llevar a cabo lo señalado se ha determinado un objetivo general que consiste en determinar la contribución de las operaciones de ciberguerra al logro de los objetivos establecidos por el nivel operacional en el conflicto ruso-ucraniano. Mientras que los respectivos capítulos que conforman la investigación tendrán cómo objetivos específicos describir el modo en que fueron empleadas las operaciones de ciberguerra por parte de la Federación de Rusia contra Ucrania; y analizar la incidencia en el nivel operacional de las operaciones de ciberguerra efectuadas por la Federación de Rusia respectivamente.

Como hipótesis de trabajo que se plantea para responder el interrogante de la investigación es que las operaciones de ciberguerra en el conflicto ruso-ucraniano contribuyen al logro de los objetivos del nivel operacional, al afectar las infraestructuras críticas de Ucrania, denegar el acceso a servidores gubernamentales, influenciar en la opinión pública del adversario, como así también afectar la moral de la población y de los combatientes.

La metodología empleada para alcanzar los objetivos y dar respuesta a la problemática planteada, será de carácter cualitativo con un diseño descriptivo para lograr comprender como las operaciones de ciberguerra contribuyen al logro de los objetivos operacionales. Para lo cual, se empleará fuentes primarias como reglamentos y publicaciones del nivel operacional y fuentes secundarias como artículos de revista, trabajos de investigación, e informes disponibles en internet los cuales sean válidos por su pertinencia con el objeto de estudio que ha motivado el desarrollo del presente trabajo de investigación. Se acudirá al análisis documental para la normativa existente en nuestro país y, al análisis bibliográfico para el resto de las fuentes descriptas.

Finalmente, la estructura formal del trabajo estará compuesta por dos capítulos que cumplimentarán los objetivos particulares establecidos y el objetivo general planteado, que permitirán dar respuesta al interrogante que motiva la presente investigación.

En el primer capítulo se identificarán las causas que dieron origen al conflicto entre la Federación de Rusia y Ucrania, y posteriormente se describirá el modo en que fue empleada la ciberguerra por parte Rusia. En el segundo capítulo se efectuará una explicación de cómo es considerada la ciberguerra por el país euroasiático, como así también una conceptualización del nivel operacional y cómo influye en este la ciberguerra en un contexto de guerra híbrida, para finalmente proceder a realizar un análisis de como las operaciones de ciberguerra y de información de Rusia inciden en el nivel operacional.

CAPÍTULO I:

Las operaciones de ciberguerra rusas en el conflicto con Ucrania

En el presente capítulo se desarrollarán las causas que dieron origen al conflicto entre la Federación de Rusia y Ucrania, seguidamente se describirán como fueron empleadas las operaciones de ciberguerra por parte del Estado Ruso contra Ucrania, en esta nueva forma de desarrollar los conflictos modernos en las denominadas guerras híbridas.

Orígenes y causas del conflicto Ruso-ucraniano

Ucrania existe como país desde el año 1991 cuando se produce la disolución de la Unión Soviética. Su ubicación geográfica le permite posicionarse en un lugar estratégico al encontrarse en el corazón de Europa. Al respecto el geógrafo y geopolítico Halford Mackinder señala que "quien domine Europa del Este dominará el Heartland, quien domine el Heartland dominará la Isla Mundial, quien domine la Isla Mundial controlará el Mundo" (Brixius, 2018).

Esto permite identificar la importancia que reviste estratégicamente poder dominar Europa del Este, región en la que se encuentra Ucrania, ya que estos territorios son de interés para muchos países entre los que se encuentra Rusia. Para Moscú, el país ucraniano no representa solamente un Estado que posee una enorme cantidad de recursos naturales sino que geoestratégicamente representa un escudo de seguridad que no desea liberar tan fácilmente ante la Unión Europea (Byllk Paraschnuck, 2018).

Por su parte el politólogo Zbigniew Brzezinski en la obra el *Gran Tablero Mundial* establecía con respecto a la importancia del país ucraniano lo siguiente

> (…) Ucrania, un espacio nuevo e importante sobre el tablero euroasiático, es un pivote geopolítico porque su propia existencia como país independiente ayuda a transformar a Rusia. Sin Ucrania, Rusia deja de ser un imperio euroasiático. Una Rusia sin Ucrania podría competir por estatus imperial, pero se convertiría en un Estado imperial predominantemente asiático (…) (Brzezinski, 1997, pág. 54)

Por tal razón desde la disolución de la Unión Soviética, el Estado ruso ha considerado al país limítrofe del oeste como una parte de su territorio. La región del Donbás es la que más le interesa, ya que se encuentra situada en el este de Ucrania y comprende los territorios de Lugansk y Donetsk. A pesar de los intereses rusos sobre su país vecino, las relaciones diplomáticas entre ambos estados siempre se han desarrollado en un contexto de cordialidad desde la disolución del Estado soviético.

Sin embargo, a finales del año 2004 y principios del 2005 en Ucrania se produce la revolución naranja, lo cual provoca una separación en las políticas de los dos países. En el país ucraniano implicó que miles de ciudadanos salieran a manifestarse en la calle, con la intención de que se produjeran unas nuevas elecciones presidenciales. En el desarrollo de las mismas el candidato ganador Yuschchenko tenía una evidente afinidad hacia la comunidad europea. Mientras que el candidato Viktor Yanukovich, era el que el gobierno ruso apoyaba, dada su manifiesta inclinación pro-rusa (Vera Daza, 2015).

De esta manera, las expectativas del pueblo ucraniano de poder adherirse a la Unión Europea y a la Organización del Tratado del Atlántico Norte (OTAN) parecían poder hacerse realidad. El máximo mandatario de Rusia interpretó a la revolución de color como un método llevado a cabo por Occidente para desestabilizar a su país (Pardo de Santayana, 2021).

Esta tendencia y mirada hacia occidente por parte del nuevo mandatario ucraniano no influiría en el poder de decisión que el gobierno ruso ejercía en las relaciones internacionales entre ambos Estados. Tal situación se debe a la dependencia económica existente, ya que las exportaciones e importaciones entre estos países eran mucho mayor que las que poseía Ucrania con la Unión Europea. Otra manera de ejercer presión por parte de la Federación Rusia fue mediante el suministro de gas, ya sea aumentando el precio o cortando el suministro de este, lo cual afectaría a una gran cantidad de países europeos que dependen de estos gasoductos.

Desde que se produjo la revolución naranja, el gobierno de Kiev intentó transmitir a Occidente que poseía líderes políticos que se mostraban a fin con las políticas desarrolladas por los miembros de la Unión Europea. Aun así, los cambios que procuraban la población ucraniana no se verían plasmados. Esto se debería a la mala situación económica, como a los escándalos de corrupción que asechaban a políticos como Yuschenko, que se vio obligado a destituir a Yulia Timoshenko, dueña de las cuatro de las seis empresas de gasoductos del país quien se desempeñaba como primera ministra (EFE, 2005).

En las elecciones presidenciales del año 2010 se impuso el candidato Viktor Yanukovich a la ex primer ministra Yulia Timoschenko. Con él como mandatario se procuró promover la Ley de Principios de la Política de Ucrania, la cual apoyaba la neutralidad del país en asuntos internacionales y proponía un acercamiento a la OTAN, a los fines de conseguir los objetivos que fijaba la ley sobre los principios de la seguridad

nacional de Ucrania. Esto significaba intenciones alejadas a la propuesta de Rusia y su Organización del Tratado de Seguridad Colectiva (OTSC), y por tal razón quedaba entre la OTAN y la OTSC, en una situación que siendo neutral en su propuesta no le garantizaba la seguridad que pudiese garantizar su soberanía, en virtud de su limitado poder militar (Vera Daza, 2015).

El Estado de Ucrania y la política de su presidente tenían las intenciones de poder adherirse a la Unión Europea, mediante el Acuerdo de Asociación, que establecía una asociación política entre ambas partes. La Unión Europea tenía la intención de poseer un suministro de gas regular, y Ucrania poder contar con capitales extranjeros y poder exportar sus productos a la comunidad europea; siendo requisito para ello que la opositora Yulia Timoschenko fuese liberada tras ser condenada a siete años de prisión por autorizar la firma del acuerdo sobre el precio y el abastecimiento de gas ruso que el actual gobierno consideraba injusto y desventajoso para Ucrania (Fernández R. , 2011).

En noviembre del 2013 se suspende el Acuerdo de Asociación ante la negativa de Kiev de liberar a Timoschenko, como así también por la presión que ejerció el gobierno de Vladimir Putin para que esté se rechazara. El Acuerdo de Asociación entre la Unión Europea y Ucrania, se convertiría en causa de conflicto si Kiev entablaba lazos con Europa y el comercio ruso-ucraniano quedaría muy limitado. Yanukovich tuvo que ceder ante tal situación y como consecuencia de esto el pueblo ucraniano se manifestó en las calles de la ciudad capitalina estallando una revolución que sería conocida como Euromaidán (Pardo de Santayana, 2021).

Estas protestas se acentuaron a comienzo del año 2014 tornándose más virulentas. Aquí las manifestaciones empezaban a ser más intensas y agresivas, e inclusive se autorizó el uso de la fuerza lo que acrecentó aún más la violencia. En febrero de 2014 la Rada Suprema destituyó al presidente ucraniano por haberse ausentado de sus funciones y su lugar fue ocupado por Oleksandr Turchínov. Ante tal situación desde Moscú no reconocían al nuevo presidente, dado que para el gobierno ruso el nuevo presidente no había sido elegido democráticamente sino mediante un golpe de Estado (Vera Daza, 2015).

Los enfrentamientos en las calles no cesaban en Ucrania y ante tal motivo Putin ordenó a sus tropas a movilizarse a la península de Crimea. Rusia tomó Crimea entre febrero y marzo de 2014 mediante el despliegue de fuerzas especiales, personal de las fuerzas armadas rusas que no usaban insignias y que serían conocidos por la opinión

pública como pequeños hombres verdes. Crimea es importante para el gobierno ruso dada su importancia geopolítica, ya que es la región que conecta a Rusia con Europa. Además, los gasoductos que van desde la Federación de Rusia hacia Europa atraviesan Crimea, por tales razones es importante destacar que al Kremlin le era conveniente hacerse con este territorio (Salmón & Rosales, 2014).

Desde el punto de vista militar el puerto de Sabastopol, ubicado en la península, era de fundamental importancia para el poderío naval ruso, no solo para la proyección en el Mar Negro sino también en el Mar Mediterráneo lo cual le permitiría proteger las líneas comerciales además de los gasoductos. Esto significaría ahorros en términos económicos ya que no debería pagar por la renta de la base y al mismo tiempo representaría una disminución o eliminación de la flota ucraniana ante un eventual conflicto militar entre ambos países (Añorve, 2016).

Pero los acontecimientos desarrollados en Crimea no serían los únicos en el que las fuerzas rusas tendrían participación. Las tropas rusas también comenzaron a movilizarse al este de la frontera de Ucrania con Rusia, en las óblast de Lugansk y Donetsk.

Ilustración 1: Óblast de Donetsk y Lugansk. Fuente: https://www.elmundo.es

Los incidentes se incrementaban al mismo tiempo en ambas regiones donde separatistas prorrusos tomaban edificios gubernamentales. Ante tales sucesos el presidente ucraniano no estaba dispuesto a permitir lo mismo que sucedió en Crimea y

acusaba a su homónimo de Rusia, Putin, de instigar y financiar los disturbios por parte de los prorruso (Sánchez-Vallejo, 2014).

Aquí también se celebraron referéndum de autodeterminación y ambas regiones se declararon independientes de Ucrania como republicas populares. Durante el desarrollo del conflicto en el este de Ucrania, el gobierno ruso apoyó con fuerzas militares y armamento a las fuerzas pro-rusas que combatieron contra las fuerzas militares ucranianas. Con estas acciones las intenciones del Kremlin era mantener a Ucrania en un conflicto constante a los fines de evitar el acercamiento con Europa y con la OTAN, a la vez que pretende hacer valer los derechos de los ciudadanos del este de Ucrania que presentan un marcado arraigo con la Federación de Rusia (Vera Daza, 2015).

Operaciones de ciberguerra desarrolladas en el conflicto

En este conflicto se desarrollaron numerosas operaciones explotando el ciberespacio. De la misma manera que sucedió en los conflictos con Estonia y con Georgia, los piratas informáticos pro-rusos efectuaron una gran variedad de ataques informáticos.

Desde mediados 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 iniciaban 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).

Los ciberataques a Ucrania comenzaron a intensificarse a partir de finales del 2013, cuando los manifestantes ucranianos daban claros indicios que no iban a renunciar y desistir de las protestas efectuadas en el Euromaidán. Los sitios web de la oposición fueron blancos de ataques de denegación de servicio distribuida –DDoS–, donde la mayoría de los cuales provenían de *botnets* –conocidos también como ejércitos de zombies– que empleaban *malwares* como Black-Energy y Dirt Jumper. Estas operaciones fueron atribuidos al grupo *hacktivista* prorruso CyberBerkut, los cuales consiguieron que los ataques DDoS duraran varias semanas algo nunca visto hasta ese momento (Pakharenko, 2015).

Otro tipo de ataque que se produjo durante el desarrollo de la revuelta en Kiev, tuvo como destinatario a los teléfonos móviles de los políticos de la oposición, que recibieron enormes cantidades de mensajes SMS –servicio de mensajes cortos– y llamadas telefónicas para evitar que se pudieran comunicar entre ellos y que de esta manera lograran coordinar algún tipo de defensas. Pero estos no serían los únicos que recibirían mensajes SMS falsos, sino que también la población que se encontraba manifestándose, a los cuales se los amenazaba con enjuiciarlos por participar en las protestas (Pakharenko, 2015).

En febrero de 2014 soldados rusos armados sin insignias, los pequeños hombres verdes, tomaron el control del Aeropuerto Internacional de Simferopol, como así también se apoderaron de la compañía telefónica y de internet Ukrtelecom en Sabastopol, ambas localidades pertenecientes a la península de Crimea. Las acciones llevadas a cabo por estas fuerzas especiales tuvieron como objetivo apoderarse de los centros de comunicaciones y manipular los cables de fibra ópticas (Azhar & Shaheen, 2015).

Al intentar aislar Ucrania de las telecomunicaciones, las fuerzas rusas debieron apuntar al terreno cibernético clave en puntos operativamente decisivos. Crimea era una de las áreas vulnerables en Ucrania, ya que solo poseía un punto de intercambio de internet que conectaba la península con el resto del país. Las fuerzas especiales rusas entendieron que, dañando o cerrando este punto de intercambio de internet, toda la región quedaría aislada, lo que le permitió a Rusia controlar las comunicaciones que allí se producían. Con ello Moscú pudo monitorear cualquier tipo de comunicación que se originara dentro o fuera de la península, lo que a su vez le proporcionó inteligencia precisa sobre las interacciones de Crimea con el resto del país. De esta manera se cumplimentaron los objetivos, ya que el aérea de interés quedó completamente aislada (Azhar & Shaheen, 2015).

Cuando las fuerzas rusas lograron ingresar en Crimea en marzo del 2014, la infraestructura de telecomunicaciones de la península ya había sido cerrada, los principales sitios de internet de Ucrania bloqueados –el principal sitio web del gobierno de Ucrania se cerró por el lapso de 72 horas– al igual que la telefonía móvil de funcionarios ucranianos. Esto demuestra que la explotación de las bondades que brinda el quinto dominio, fue importante para que la Federación de Rusia pudiese avanzar sobre el país limítrofe y de esta manera consolidar la anexión de Crimea (Pakharenko, 2015).

Como medida de lo sucedido desde Kiev decidieron cortar los vínculos de comunicación entre Ucrania y el territorio en manos rusas. A pesar del esfuerzo la conectividad se mantuvo sin restricciones, lo que posibilitó que los servicios de seguridad de Rusia pudieran tener acceso a los sistemas internos para recopilar datos para efectuar inteligencia y efectuar otros tipos de operaciones de información. Al mismo tiempo que los medios de comunicación, como las redes sociales participaban en la difusión de propaganda a favor de Rusia.

Cuando el conflicto se trasladó hacia al este de Ucrania, el ciberespacio desempeño un papel trascendental para el desarrollo de las operaciones militares. Los ataques físicos destruyeron el cableado, la infraestructura de transmisión, lo que ocasionó el aislamiento de la población de los medios de comunicaciones. Las acciones militares fueron ejecutadas con difusión y propaganda en canales de televisión rusos y medios de internet. Las tareas de inteligencia de señales, al igual que el ciberespionaje posibilitaron llevar adelante el desarrollo de operaciones eficaces contra el ejército ucraniano (Pakharenko, 2015).

Equipos de *hackers* identificados con el gobierno de Moscú como APT-29, también conocidos como Cozy Bear, operaban enviando correos electrónicos *spear phishing* con la finalidad de obtener información valiosa para inteligencia mediante el ciberespionaje. Este tipo de correos electrónicos funcionan adjuntando un archivo malicioso o un enlace a una descarga de un *malware*, que crean una puerta trasera como lo es el denominado Hammertoss, que es capaz de evadir su detección en virtud de su capacidad para imitar el comportamiento de usuarios legítimos (Weedon, 2015).

En lo referente a la guerra de la información, está siempre ha estado relacionada con las operaciones militares convencionales y en este conflicto no sería la excepción. Rusia controló el flujo de la información, donde las operaciones se extendieron por todo el espectro de comunicación en el dominio cibernético abarcando los tres niveles: físico, lógico, y social (Jaitner, 2015).

Las acciones desarrolladas por grupos de *hackers* –acceso a grabaciones telefónicas, correos electrónicos, ataques a páginas web gubernamentales y portales de noticias– posibilitaron obtener superioridad en el flujo y manejo de información, lo cual dificultó al gobierno y a las fuerzas ucranianas poseer un análisis situacional correcto de lo que acontecía en Crimea, afectando de esta manera el proceso de toma de decisiones.

Otra de las contribuciones que efectuó la explotación del ciberespacio en el conflicto con Ucrania fue en la utilización de la propaganda en las operaciones psicológicas, y en la mencionada guerra de información a través del empleo de internet y de las redes sociales. Desde el entorno cibernético se producen ataques donde se presenta información manipulada con la intención de afectar la percepción de la situación y el proceso de toma de decisiones para inducirlo a tomar de manera voluntaria una decisión predeterminada por el emisor para ejercer un control reflexivo (Lange-Ionatamishvili & Svetoka, 2015).

Rusia en mención de lo descripto ha hecho uso de ciberataques sociales que se explotaron de manera organizada mediante el empleo de redes sociales. Estas redes normalmente se basan en la confianza dado a que se conforman con grupos de personas que comparten ideas afines. El componente clave de esta herramienta cibernética, lo constituye la narrativa que lo impulsa, en la cual la difusión de rumores es una de las tácticas más efectivas junto con la difusión de información manipulada. El grupo CyberBerkut hackeó las vallas publicitarias de las redes sociales antes de las elecciones parlamentarias de Ucrania difundiendo videos de políticos que eran etiquetados como criminales de guerra. En las redes sociales los hackers prorrusos han sembrado el miedo, la ansiedad y el odio entre la población de etnia rusa de Ucrania. Han manipulado y distribuido imágenes de atrocidades cometidas por el ejército ucraniano, como fosas de personas torturas, reclutamiento de niños soldados, y uso de armas contra civiles entre otras (Lange-Ionatamishvili & Svetoka, 2015).

En contra oposición a lo anterior este tipo de técnica también fue empleada para acompañar las acciones desarrolladas por las fuerzas de operaciones especiales rusas, al difundirse imágenes en las redes sociales de los pequeños hombres verdes posando junto a madres con niños y con ancianos (Lange-Ionatamishvili & Svetoka, 2015). Esto demuestra que este tipo de operaciones apoya a las acciones militares, ya que permite manipular la percepción y la toma de decisiones en la población.

Durante este conflicto se han empleado ciberataques para producir efectos cinéticos, al producirse el primer ataque a la red eléctrica de otro país. La capacidad cibernética de los hackers rusos posibilitó llevar adelante un ataque sofisticado para poder dañar la infraestructura crítica de Ucrania.

El 23 de diciembre de 2015 la empresa ucraniana de distribución eléctrica Kyivoblenergo, sufrió un ciberataque que dejo aproximadamente alrededor de 225.000

clientes sin electricidad. Este ataque afectó partes adicionales de la red de distribución y los operadores se vieron obligados a cambiar su funcionamiento a modo manual. El suministro eléctrico se cortó entre una y seis horas, pero los centros de distribución no estuvieron en pleno funcionamiento operativo después de transcurridos varios meses (Shehod, 2016).

Este ataque fue minuciosamente estudiado y planificado, ya que comenzó a gestionarse en marzo de ese año, donde la incursión inicial a la red fue con correos electrónicos que contenían el *malware* BlackEnergy. Este *malware* creó una comunicación con el canal de mando y control del adversario, permitiendo recopilar información del sistema infectado. Los hackers recopilaron credenciales y se movieron a través de la red para pivotar hacia los segmentos de red donde existían las estaciones de trabajo y servidores de despacho de supervisión, control y adquisición de datos –SCADA. También obtuvieron acceso a las credenciales de la red privada virtual –VPN– que posibilitaba el acceso a la red SCADA, que permitió coordinar el ataque (Shehod, 2016).

Las consecuencias de este ataque son las que los *hackers* habían planificado, ya que no solo lograron la interrupción eléctrica en la población, sino que también lograron que los operadores no pudieran acceder al sistema para restablecer el funcionamiento nuevamente. Este procedimiento fue acompañado por ataques de denegación de servicio telefónico –TDoS– al centro de llamada de atención a los clientes con miles de llamadas falsas para evitar que las personas que llamaban legítimamente pudieran informar de la interrupción del servicio eléctrico (Shehod, 2016).

Finalmente, es posible observar que las operaciones de ciberguerra empleadas por la Federación de Rusia en el conflicto con Ucrania, abarcaron un amplio campo de acciones y objetivos. Ya que permitieron tener acceso a información secreta del gobierno ucraniano mediante el ciberespionaje; influir en proceso de toma de decisiones de las autoridades gubernamentales como del ejército mediante el control reflexivo u operaciones psicológicas; y afectar las páginas oficiales del gobierno ucraniano. Además de ello, también posibilitaron aislar a la península de Crimea de los medios de comunicación mientras se producía su anexión; efectuar operaciones de información con el empleo de las redes sociales para manipular la percepción de los acontecimientos de los hechos en la sociedad; y producir efectos cinéticos como lo es el ataque a la infraestructura crítica.

CAPÍTULO II:

La ciberguerra y su incidencia en el nivel operacional

En el presente capítulo se efectuará una descripción de cómo es concebida la ciberguerra para la Federación de Rusia, como así también una conceptualización del nivel operacional en el contexto de la guerra híbrida y cómo influye en ella la ciberguerra, para posteriormente analizar cómo las operaciones desarrolladas en el quinto dominio durante el conflicto ruso-ucraniano inciden para contribuir al logro de los objetivos propuestos por este nivel de la conducción.

La concepción de la ciberguerra para la Federación de Rusia

La capacidad cibernética que posee la Federación de Rusia, permite posicionarla como una de las principales potencias mundiales líderes en la explotación del ciberespacio. Esto se debe a la gran experiencia que tiene en el desarrollo de guerra híbridas y de operaciones especiales, donde tiene un mayor ejercicio en el campo de la guerra cibernética.

El Estado ruso ha efectuado una importante inversión en capacidades cibernéticas a partir de la primera década del año 2000. Desde entonces la herramienta internet se ha convertido en una importante arma para los conflictos del siglo XXI. El pilar de esto lo constituye la Doctrina de Seguridad de Información, firmada por el presidente Putin ese mismo año; y por la nueva Doctrina promulgada en el año 2016 mediante Decreto Nº 646, que deja sin efecto la mencionada anteriormente (Raychev, 2019).

En este nuevo Decreto se menciona el objetivo estratégico de garantizar la seguridad de información en el campo de la defensa ante amenazas de origen interno y externo asociadas al uso de tecnologías de la información. Además, establece la necesidad de mejorar el sistema de seguridad de la información de las Fuerzas Armadas de la Federación de Rusia, que incluye a las fuerzas y medios de la guerra de la información (Decreto Nº 646, 2016).

Conforme a lo mencionado con anterioridad el Estado ruso al igual que sus fuerzas militares han sabido integrar la guerra cibernética con la guerra de la información. Para el ejército ruso estás resultan inseparables y deben ser acompañadas durante el desarrollo de una campaña con operaciones militares. Sin embargo, es importante destacar que para los politólogos rusos y militares especialistas la ciberguerra es conceptualizada dentro de un campo más amplio que es el de la guerra de la información. Este es un concepto de

características holísticas que incluye a las operaciones de redes informáticas, guerra electrónica, operaciones de información y operaciones psicológicas (Connell & Vloger, 2017).

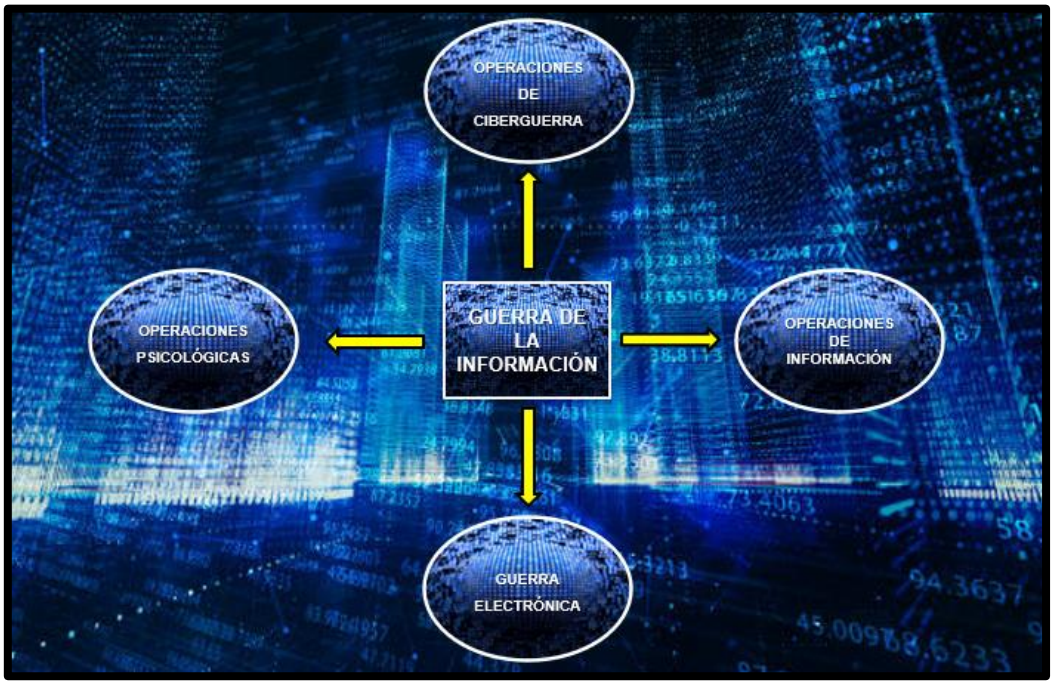

Ilustración 2. Concepción de la Guerra de la Información para Rusia. Elaboración propia. Fuente: Connell & Vloger.

Según la doctrina militar de la Federación de Rusia del año 2010, una de las características esenciales de los conflictos militares modernos es el empleo previo de medidas de guerra de información con el fin de poder alcanzar los objetivos establecidos por el poder político sin la utilización del poder militar. Por esta razón la guerra de la información, y por ende las ciberoperaciones, son una herramienta a disposición del Estado para su aplicación tanto en tiempo de paz como en tiempos de guerra (Connell & Vloger, 2017).

Los pensadores militares rusos consideran que la explotación de la guerra de la información puede ser aplicada para desestabilizar gobiernos, engañar adversarios, influir en la opinión pública y reducir el espíritu combativo de los enemigos. La explotación del ciberespacio con operaciones como las descriptas posibilitan alcanzar los objetivos que sean propuestos. Asimismo, su implementación antes del inicio de las operaciones militares convencionales permite preparar el ambiente en el cual se desarrollarán las hostilidades (Connell & Vloger, 2017). Otra conclusión a la que han arribado los analistas militares es el de la analogía entre el empleo de las distintas operaciones que conforman

a la guerra de la información en los conflictos modernos con el de los medios de destrucción masiva del siglo pasado. La nueva carrera armamentista consiste en desarrollar nuevos software y sistemas de información que sean mejores y superiores a los de otros países (Vicente, 2011).

El análisis y posterior enseñanza que dejó en materia de empleo de ciberoperaciones el enfrentamiento con Georgia en el año 2008, motivó a que el Ministerio de Defensa anunciase la creación de unidades capacitadas para el la ejecución de este tipo de operaciones y principalmente de operaciones de información. Sin embargo, esta idea fue modificada en 2013, dado a que se decidió crear una unidad cibernética en el ejército para que estuviese a cargo de las operaciones cibernéticas ofensivas y defensivas como así también de la investigación cibernética (Raychev, 2019).

Aun así, además de las capacidades militares existentes para la ejecución de este tipo de acciones, el gobierno ruso ha tomado la decisión de contratar a expertos operadores cibernéticos para la participación en las operaciones de esta nueva modalidad de llevar adelante sus conflictos contra otras naciones. Los *hackers*, constituyen un elemento fundamental para los intereses de Rusia en función de que estos son idóneos para actuar en la zona gris de la guerra de la información. Con esto es dable observar cómo el gobierno emplea tanto herramientas estatales como no estatales que caracterizan a la guerra híbrida llevada adelante por este país.

El nivel operacional y la ciberguerra como herramienta de la guerra híbrida

La publicación conjunta *PC 20-01 Planeamiento para la Acción Militar Nivel Operacional* en su versión Experimental del año 2019, estable que son tres los niveles de conducción y de planificación de un conflicto bélico: el nivel estratégico –nacional y militar–, el nivel operacional y finalmente el nivel táctico. El nivel operacional es aquel que se caracteriza por articular medios y fines a los efectos de poder alcanzar el Estado Final Operacional, el cual deberá ser a fin a los objetivos que persigue la estrategia militar, que a su vez posibilitaran conseguir los objetivos establecidos por la estrategia nacional, en otras palabras, los de la conducción política del Estado.

También establece que este nivel es el responsable de establecer una conexión entre el nivel estratégico militar con el nivel táctico. Eso implica que el nivel operacional debe traducir el cómo se llevará adelante lo solicitado por el nivel estratégico para que el nivel táctico lo comprenda y lo ejecute en el teatro de operaciones. Para ello el

comandante debe traducir el Estado Final de los niveles superiores en Estados Finales Operacionales.

Para alcanzar el Estado Final Operacional, deben cumplimentarse los objetivos propuestos por el nivel operacional. Estos objetivos que permite alcanzar la situación deseada en este nivel de la conducción se denominan objetivos operacionales.

Estos conceptos descriptos no han sido estáticos a lo largo de la historia en los enfrentamientos entre Estados, sino que estos han ido adaptándose conforme a los avances de la humanidad y de la tecnología. Por tal razón el arte operacional con el cual el comandante operacional planifica la ejecución de las campañas para alcanzar los objetivos también se ha visto en constante evolución.

En los conflictos modernos las guerras híbridas han tomado una gran dimensión en los últimos años y países como la Federación de Rusia se ha convertido en un especialista en el desarrollo de este tipo de enfrentamientos. Este país ha sabido adaptar el arte operacional a todos los medios disponibles para alcanzar los objetivos que posibiliten lograr el estado final.

La nueva manera de desarrollar los conflictos por Rusia ha llevado a la necesidad de adecuar el concepto de batalla profunda, la cual es una estrategia que ha estado presente desde comienzo de siglo XX en la doctrina militar rusa (Campos Robles, 2018). La batalla en profundidad posibilita el desarrollo de las operaciones en todos los dominios existentes para dar forma a las acciones antes del conflicto utilizando métodos híbridos en múltiples dominios con la finalidad de crear ventajas.

Otro concepto que Rusia emplea en los enfrentamientos con otros países es el de control reflexivo que es similar a lo que del Departamento de Defensa de Estados Unidos denomina como operaciones psicológicas (San Martin, 2018).

El control reflexivo tuvo su origen en los años sesenta en la ex Unión Soviética, y tiene como finalidad influir en la forma en que el enemigo percibe la realidad, sus planes y en la forma que actuará, a los efectos de poder imponerse a su voluntad (Martinez Pontijas, 2020).

Este procedimiento combina la guerra de la información y las operaciones de información para alcanzar efectos en los niveles estratégicos, operacional y táctico. De esta manera el avance tecnológico y la explotación del quinto dominio ha sido determinante para expandir el alcance de los conflictos, creando de esta manera una

amenaza aún más híbrida. El empleo de las herramientas que brinda el ciberespacio no solo aumenta la eficacia y la eficiencia del control reflexivo, sino que también posibilita brindar información al adversario para que cambie y adopte la postura que se desea que este tome (Bachman, 2021).

En el pensamiento estratégico de Rusia se considera que la guerra cibernética es un elemento esencial en las fases iniciales de un conflicto, ya que la superioridad de la información es fundamental, dado a que puede utilizarse para para influir en la voluntad, capacidad o en la resolución militar o política para emprender un enfrentamiento. De esta manera la guerra cibernética está destinada a ser utilizado como parte de la guerra híbrida, en conjunción con otros elementos de influencia para dar forma al curso político de un enfrentamiento. Esto permite lograr la superioridad de información en todos los niveles y configurar las operaciones a desarrollar en todas las etapas del conflicto (Kristiansen & Hoem, 2021).

Así es posible observar como el arte operacional de los comandantes rusos ha ido evolucionando desde su origen y ampliando sus herramientas conforme a la aparición de nuevas tecnologías y de la explotación de nuevos dominios como lo es el ciberespacio. El ciber ha permitido desarrollar estrategias que han estado presente en su doctrina militar como son los conceptos de batalla profunda y el control reflexivo, los cuales en la actualidad son aplicados en esta manera híbrida de llevar adelante sus enfrentamientos contra otros países.

Las operaciones rusas en Ucrania desde la óptica del nivel operacional

Durante el desarrollo de este conflicto queda en evidencia la capacidad que el Estado ruso demuestra para emplear operaciones cibernéticas y de información con la finalidad de conseguir el logro de los objetivos militares como políticos. Es de esta manera, como mediante la explotación del quinto dominio desarrolla un amplio abanico de opciones que contribuyen a conseguir los efectos deseados.

Estableciendo una analogía con el concepto de batalla profunda desarrollada por los ejércitos de la ex Unión Soviética, se puede establecer que en este conflicto se opera con las características propias de este, ya que posibilita crear una articulación entre tiempo y espacio para emplear de manera efectiva las fuerzas terrestres con operaciones especiales. Para lograr esa sinergia necesaria para el desarrollo de las operaciones el empleo del ciberespacio crea ventanas de oportunidad para que ello sea factible.

Las capacidades cibernéticas que fueron empleadas posibilitaron a la Federación de Rusia lograr una serie de efectos de gran relevancia, donde desde el punto de vista del nivel operacional el empleo de un número mínimo de tropas articuladas con operaciones cibernéticas integradas posibilitó obtener una ventaja operativa sobre las fuerzas ucranianas. Al mismo tiempo permitió a la conducción rusa mantener una negación de los eventos sucedidos en Ucrania donde las operaciones ciberguerra y de información permitieron retrasar la opinión como así también la intervención internacional (Greenberg, 2017).

Las principales operaciones rusas en Ucrania consistieron en operaciones de configuración de información, operaciones cibernéticas para interrumpir y negar el mando y control del país ucraniano, operaciones de fuerzas especiales integradas para apoderarse del terreno físico y cibernético, y operaciones de ciberespionaje para obtener una ventaja desde el punto de vista operacional y táctico. La guerra de información, con operaciones de ciberguerra y de información principalmente, permitió antes del inicio de las operaciones de combate entre las fuerzas terrestres crear una parálisis estratégica en los niveles de conducción de Ucrania cómo así también en la comunidad internacional, lo cual posibilitó que la conducción del nivel operacional se apoderará de un territorio clave, cómo lo era Crimea para el Estado ruso, y que originará una campaña de información viable para apoyar esas operaciones (Sprang, 2018).

Las operaciones cibernéticas y de información permitieron establecer las condiciones necesarias para que las fuerzas de operaciones especiales pudiesen avanzar hacia la anexión de Crimea, ya que facilitaron la creación de efectos entre los demás dominios a través del ataque de la infraestructura critica de internet de Ucrania, donde las fuerzas terrestres aislaron la infraestructura de telecomunicaciones como también de internet (Tsipis, 2014).

El ciberespionaje ha obtenido de inteligencia que resultó valiosa para proporcionar información sobre la planificación y las operaciones del gobierno, del ejército y de las fuerzas del orden de Ucrania. Esta inteligencia fue empleada para poder maniobrar y otorgar ventaja a los separatistas prorrusos (Lewis, 2015).

Las capacidades cibernéticas fueron una herramienta eficaz a nivel operacional para crear una parálisis en la arquitectura de comando y control del oponente. Estratégicamente proporcionó lapsos de tiempo de ventaja a través de una narrativa estratégica y de operaciones de información coordinadas para evitar que la comunidad

internacional comprendiera el ambiente operacional, lo cual posibilitó que las operaciones cibernéticas pudiesen crear tiempo y espacio principalmente en el nivel operacional y táctico (Sprang, 2018).

Las acciones rusas demostraron la evolución de su arte operacional en el desarrollo de conflictos modernos, conocidos en occidente como guerra híbrida. El empleo eficiente y eficaz del ciberespacio posibilitó generar tiempo y espacio en los tres niveles de la conducción en la que se desarrolló el conflicto. Las operaciones de ciberguerra permitieron impactar en todos los niveles del sistema ucraniano afectando la toma de decisiones y de comando y control. Las capacidades cibernéticas integradas a las de información lograron un impacto en el nivel estratégico que hasta este conflicto no tenía precedente alguno, lo cual dificultó la comprensión de los acontecimientos por parte del plano internacional y afectó en gran medida la capacidad de respuesta por parte de occidente. Los resultados logrados fueron indispensables para establecer las condiciones de la maniobra operacional, como las operaciones del nivel táctico que dieron lugar a que las fuerzas de operaciones especiales rusas tomaran rápidamente un territorio clave como lo era la península de Crimea (Sprang, 2018).

El control reflexivo ha permitido una integración significativa en los niveles estratégicos y operacional, para que la Federación de Rusia pudiese alcanzar el estado final deseado en Ucrania para controlar Crimea. Expertos en el conflicto ruso-ucraniano identificaron los siguientes elementos claves de la técnica de control reflexivo rusa empleadas contra Urania: 1) operaciones de negación y engaño para ocultar la presencia de las fuerzas rusas en Crimea, como las de las fuerzas de operaciones espaciales, los pequeños hombres verdes sin insignias, 2) el esfuerzo efectuado para dar forma a la narrativa sobre los acontecimientos sucedidos en el conflicto a través de los medios de comunicación tradicionales y fundamentalmente de las redes sociales (Snegovaya, 2015).

Una herramienta de las capacidades cibernéticas que resultó esencial para el control reflexivo fue el uso eficiente del ciberespionaje llevado adelante por los *hackers* rusos, para obtener inteligencia a los fines de poder comprender los planes del enemigo en detalles. Esto posibilitó adelantarse a las intenciones de las fuerzas ucranianas en lugar de actuar en respuesta a sus acciones.

Cuando las capacidades cibernéticas se emplean de manera sincronizada como es el caso con las fuerzas de operaciones especiales, posibilitan que el comandante del nivel operacional pueda planificar las operaciones por desarrollarse, y fundamentalmente

manejar y controlar el ritmo o tempo de las operaciones entre las distintas fuerzas que operan en el conflicto. Las operaciones rusas en el conflicto con Ucrania fueron una demostración de los beneficios que el nivel operacional obtuvo de las operaciones de ciberguerra y de información para obtener ventajas y explotar sinergias entre los distintos elementos que participaron en el conflicto. De esta manera fue posible reducir el riesgo y aplicar el poder de combate en puntos críticos decisivos, empleando un enfoque indirecto para atacar al centro de gravedad del oponente. Las herramientas cibernéticas empleadas evitaron la culminación rusa y por consiguiente esto obligó al enemigo a realizar operaciones costosas más allá de su alcance operacional (Sprang, 2018).

Al emplearse las capacidades cibernéticas en todos los dominios proporcionan al comandante del nivel operacional de dos factores esenciales como ser el tiempo y espacio para la defensa los cuales permiten exponer y aumentar la vulnerabilidad del enemigo al obligarlo a concentrar sus fuerzas. Los rusos emplearon eficazmente las capacidades cibernéticas defensivas mediante operaciones de información para evitar que organismos como la OTAN o países alineados a Ucrania interfieran en las operaciones. Para ello llevaron adelante una defensa cibernética estratégica mediante la utilización de operaciones de ciberguerra y de información, mientras efectuaban operaciones ofensivas con las fuerzas de operaciones especiales para apoderarse del territorio clave durante el inicio de las operaciones terrestres (Sprang, 2018).

Este conflicto ha demostrado que el uso de las operaciones de ciberguerra y de las operaciones de información junto con las herramientas que estas brindan, posibilitaron crear condiciones para asumir la iniciativa en un conflicto actuando bajo los principios de guerra como la concentración o masa.

Para Sprang (2018) la explotación del ciberespacio permite simultaneidad y alcanzar profundidad cuando se emplea en forma sincronizada con los otros dominios. Es de esta manera que la sinergia alcanzada entre los dominios proporcionó una amplia gama de opciones al comandante operacional, creando confusión, y retraso en el ciclo de tomas de decisiones del adversario, y permitiendo mantener la iniciativa, lo que obligó a la culminación operativa del oponente. Al mismo tiempo que establece que las operaciones de Rusia en Ucrania han aplicado el arte operacional para articular el nivel táctico con el estado final estratégico deseado por el gobierno de Moscú. Las operaciones cibernéticas y de información son esenciales en los conflictos actuales, dado a que posibilitan a los

comandantes del nivel operacional la oportunidad de dar lugar a la batalla profunda y controlar el ritmo de las operaciones en los conflictos de naturaleza híbrida.

Finalmente se puede establecer que las operaciones en el ámbito del dominio cibernético, cómo las efectuadas por la Federación de Rusia a Ucrania permitió que la población acogiera a las tropas rusas. La combinación de estas acciones con las fuerzas de operaciones especiales, quebrantaron la moral de las fuerzas ucranianas, lo que provocó la rendición de unos dieciséis mil soldados (Derleth, 2021). Además, Rusia pudo manipular la percepción de la población ucraniana, impedir una respuesta militar, fomentar la desconfianza en el gobierno a través de la propaganda mediante redes sociales e influir en el proceso de toma de decisiones en todos los niveles de conducción del país ucraniano.

CONCLUSIONES

Este trabajo de investigación sobre las operaciones de ciberguerra llevadas adelante por la Federación de Rusia en el conflicto contra Ucrania, se inició mediante la descripción de como las amenazas de los conflictos actuales son de características híbridas, en el cual intervienen tanto actores estatales como no estatales. Siendo aquí donde la explotación del dominio cibernético toma especial relevancia para producir efectos en un ambiente operacional cada vez más complejo a los fines de alcanzar el estado final deseado.

A continuación de ello se formuló el interrogante que diera respuesta a la problemática planteada, siendo este: ¿cómo contribuyen las operaciones de ciberguerra desarrolladas por la Federación de Rusia en el conflicto con Ucrania al logro de los objetivos operacionales? Seguidamente se estableció el objetivo general para el desarrollo de la investigación el cual consiste en: determinar la contribución de las operaciones de ciberguerra al logro de los objetivos establecidos por el nivel operacional en el conflicto ruso-ucraniano.

A los fines de dar respuesta a la problemática planteada se desarrollaron dos capítulos que correspondían a cada objetivo particular establecido, los cuales fueron alcanzados en su totalidad.

En el desarrollo del primer capítulo fue posible observar las causas que dieron origen al conflicto entre estos dos Estados pertenecientes a la ex Unión Soviética. En ellas pudo contemplarse el interés existente por parte del Estado y del pueblo ucraniano de acercarse a la Unión Europea mediante un Acuerdo de Asociación, lo cual fue determinante para que Rusia se opusiera a ello ejerciendo presión para que esto no ocurriera.

Para Moscú las relaciones con su país limítrofe eran esenciales dado a que representa un perímetro de seguridad con occidente, es decir con la OTAN; como así también por las negociaciones y relaciones económicas existentes entra ambos Estados. Un aspecto importante, es la relevancia que reviste geopolíticamente Crimea ya que permite la conexión entre el país euroasiático y Europa.

Desde una perspectiva militar la península resultaba fundamental para los intereses de Rusia no sólo en el Mar Negro, sino también en el Mar Mediterráneo para la

protección de su poderío naval, como así también para proteger las líneas comerciales y también los gasoductos que atraviesan de Rusia al continente europeo.

A los fines de poder alcanzar sus intereses y objetivos contra su país limítrofe, la Federación de Rusia efectuó e hizo un eficiente usufructo de las bondades que brinda el quinto dominio. En tal sentido las operaciones cibernéticas como de información se comenzaron a efectuar a finales del año 2013, cuando el pueblo ucraniano se manifestó en las calles ante la imposibilidad de poder adherirse al Acuerdo de Asociación con la Unión Europea. Rusia demostró poseer un amplio abanico de herramientas que se emplearon mediante la explotación del ciberespacio.

Las operaciones de ciberespionaje fueron esenciales para obtener inteligencia de del gobierno como así también de sus fuerzas armadas y de seguridad. Los ataques de denegación DDoS de servicios a los sitios web de autoridades ucranianas fueron importantes para que estos no tuviesen acceso a su información. Políticos como así también la población serían víctimas de enormes cantidades de mensajes de textos –SMS– en sus teléfonos móviles; a los primeros impidió de poder coordinar algún tipo de defensa, mientras que los ciudadanos recibieron amenazas por participar de las protestas del Euromaidán.

Las fuerzas de operaciones especiales en Crimea llevaron a cabo acciones que facilitó aislar la península del resto de Ucrania, al dañar y controlar el punto de intercambio de internet, lo cual posibilitó controlar todas las comunicaciones que se producían. Mientras que las operaciones militares efectuadas en la región del Donbás fueron acompañadas con operaciones de información como la difusión y la propaganda a través de medios de internet.

Los hackers prorrusos tuvieron una participación relevante al permitir obtener superioridad en el manejo y calidad de la información, lo cual dificultó a las autoridades de gobierno como a las fuerzas militares poder efectuar un análisis situacional correcto de los acontecimientos, lo que se pudo ver reflejado en el proceso de toma de decisiones. Este proceso esencial e inherente a la conducción de todos los niveles, se encontró manipulado por la narrativa de la propaganda empleada mediante la explotación de las redes sociales a través de procedimientos de control reflexivo.

Las capacidades de los hackers rusos permitieron afectar la infraestructura crítica de Ucrania al atacar a una empresa de distribución de energía, demostrando que mediante

el empleo de ciber ataques se pueden lograr efectos cinéticos, ya que el suministro de eléctrico se vio afectado por el lapso de varias horas, lo que sin dudas afectó a la población de la región ante la imposibilidad de contar con un servicio esencial y sin poder conocer cuando se restablecería el servicio en función de los ataques de denegación de servicio telefónico TDoS que sufrió la compañía prestadora del servicio.

En el segundo capítulo desarrollado se ha efectuado una descripción de como considera la Federación de Rusia a las operaciones de ciberguerra, donde estas conforman parte constitutiva de la guerra de la información junto con las operaciones de información, guerra electrónica y control reflexivo u operaciones psicológicas.

A los fines de poder analizar como inciden en el nivel operacional las operaciones de ciberguerra efectuadas por Rusia, es importante señalar que este país se ha convertido en un especialista en el desarrollo de conflictos híbridos. Para ello ha sabido adaptar el arte operacional de sus comandantes a todos los medios disponibles para alcanzar los objetivos que permitan lograr el estado final. Conceptos como el de batalla profunda y control reflexivo se han adecuado a la aparición de nuevas tecnologías y a la explotación de nuevos dominios como lo es el ciberespacio.

Precisamente en este conflicto objeto de análisis, se operó con las características del concepto de batalla profunda, dado a que permitió crear una articulación de los factores tiempo y espacio para el empleo efectivo de las fuerzas terrestres con operaciones especiales. El empleo del ciberespacio estableció ventanas de oportunidad para lograr la sinergia necesaria para el desarrollo de las operaciones tanto en el nivel estratégico como operacional.

Las capacidades cibernéticas rusas lograron efectos de gran relevancia, permitiendo que el nivel operacional mediante la integración de un número reducido de tropas con operaciones cibernéticas pudiese obtener ventajas sobre las fuerzas ucranianas. Asimismo, las operaciones de ciberguerra y de información lograron retrasar la opinión como la intervención por parte de otros países u organismos al no tener un conocimiento claro y preciso de la situación reinante.

Los datos de inteligencia obtenidos del ciberespionaje proporcionó información sobre la planificación y las operaciones del gobierno, del ejército y de las fuerzas de seguridad ucranianas. La guerra de información creó una parálisis estratégica en los

niveles ucranianos, que fue fructífera para que la conducción del nivel operacional anexara la península de Crimea.

Los ataques rusos efectuados en este conflicto han demostrado la evolución del arte operacional ruso para afrontar las guerras modernas o guerras híbridas, ya que el empleo de las herramientas cibernéticas creó tiempo y espacios en los todos los niveles de conducción, lo cual se tradujo en un impacto operativo en los sistemas ucranianos para la toma de decisiones como también de comando y control. El concepto de control reflexivo llevado adelante a través de la narrativa difundida por medio de redes sociales logró integrar los niveles estratégico y operacional para que la Federación de Rusia pudiese alcanzar el estado final deseado en Ucrania para controlar Crimea y limitar la interferencia de organismo como la OTAN o países alienados a Ucrania.

Se puede establecer que las operaciones de ciberguerra y de información efectuadas por Rusia en este conflicto han contribuido para que el nivel operacional pueda articular el nivel táctico con el estado final estratégico deseado por la conducción política de Rusia; constituyéndose las operaciones desarrolladas en el dominio cibernético esenciales para el desarrollo de los conflictos actuales, dado a que otorgan a los comandantes del nivel operacional la oportunidad de dar lugar a la batalla profunda y controlar el ritmo de las operaciones.

Finalmente, en función de las descripciones efectuadas se da cumplimiento al objetivo general establecido para el desarrollo del presente trabajo; pudiéndose comprobar que la hipótesis planteada, se ha podido corroborar y demostrar, razón por lo cual es dable establecer que la misma resulta válida.

BIBLIOGRAFÍA

Añorve, D. (2016). La Anexión de Crimea: Una respuesta a la crisis demográfica de la Fdereración Rusa. *Foro Internacional, Vol LVI, No 225 (Año 2016)*, 578-613. Obtenido de https://forointernacional.colmex.mx/index.php/fi/article/view/2329

Ayerve, P. H. (2019). La guerra de cuarta generación y las amenazas asimétricas . *Política y Estrategia*, 93-113.

Azhar, U., & Shaheen, G. (2015). *Brandishing the cybered bear: Information war and the Russia-Ukraine conflict.* Obtenido de Military Cyber Affairs: https://digitalcommons.usf.edu/mca/vol1/iss1/7/

Azhar, U., & Shaheen, G. (Volumen 1, Número 1, Artículo 7 de 2015). *BRANDISHING THE CYBERED BEAR: INFORMATION WAR AND THE RUSSIA-UKRAINE CONFLICT.* Obtenido de Military Cyber Affairs: https://scholarcommons.usf.edu/mca/vol1/iss1/7

Bachman, B. (25 de Marzo de 2021). *Hybrid: An Adjective Describing the Current War.* Obtenido de Small Wars Journal: https://smallwarsjournal.com/jrnl/art/hybrid-adjective-describing-current-war

Bilyana, L., & Cheravitch, J. (2020). The past, presente, and future of Russia´s cyber strategy and forces. En N. C. Publications, *12th International Conference on Cyber Conflict - 20/20 Vision: The Next Decade* (págs. 129-155). ESTONIA: NATO CCDCOE Publications.

Blank , S. (2017). Cyber war and information war à la russe. En G. Perkovich , & A. E. Levite, *UNDERSTANDING CYBER CONFLICT: FOURTEEN ANALOGIES* (págs. 81-98). Georgetown University Press.

Brixius, M. (2018). *El pensamiento geopolítico en la actualidad: en el uso y adaptación de la teoría del hertland en la política exterior de Vladimir Putin.* Obtenido de Universidad de San Andrés: http://hdl.handle.net/10908/16516

Brzezinski, Z. (1997). *El gran tablero mundial.* Washington, D.C.: Paidós.

Byllk Paraschnuck, L. (2018). Origenes del conficto ucraniano. *Revista Aequitas -Estudios sobre historia, derecho e instituciones-*, 155-177.

Campos Robles, M. (2018 de Marzo de 2018). *El Arte Operacional Ruso: de Tukhachevsky a la actual ´Doctrina Gerasimov`*. Obtenido de Instituto Español de Estudios Estrategicos: http://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO35-2018_Arte_Operacional_Rusia_MiguelCampos.pdf

Clark, B. R. (2010). Las operaciones de información como elemento disuasivo para el conflcito armado. *MILITARY REVIEW*, 1-11.

Connell, M., & Vloger, S. (marzo de 2017). *Russia´s approach to cyber warfare.* Obtenido de CNA - Analysis & Solutions: https://www.cna.org

Crespo, G. M. (2018). Características del planeamiento operacional en el marco de la defensa ante una amenaza híbrida. *Trabajo Final Integrador*. CABA, Argentina: Escuela Superior de Guerra Conjunta.

Cuenca, A. (07 de 11 de 2019). *Crimea, una península por se enfrentan imperios.* Obtenido de El Orden Mundial: https://elordenmundial.com/crimea-una-peninsula-por-la-que-se-enfrentaron-imperios/

de Santayana Gomez de Olea, J. P. (25 de 07 de 2018). *Consideraciones estratégicas de la reforma militar rusa.* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/

Decreto 457/2021. (14 de Julio de 2021). Directiva de Política de Defensa Nacional. Apruébase actualización. Buenos Aires, Argentina.

Decreto Nº 646. (05 de 12 de 2016). *Decreto del Presidente de la Federación de Rusia del 5 de diciembre de 2016 N 646 "Sobre la aprobación de la Doctrina de seguridad de la información de la Federación de Rusia"*. Recuperado el 03 de Agosto de 2021, de http://base.garant.ru/71556224/#friends

Derleth, J. (2021). La Guerra de nueva generación de Rusia: Disuadir y ganar en el nivel táctico. *Military Review*, 13-26. Obtenido de https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/2Q-2021/Derleth-SPA-Q2-2021-A.pdf

EFE. (09 de 09 de 2005). *Los escándolos de corrupción llavan a Yushchenko a destituir al gobierno.* Obtenido de El Mundo.es: https://www.elmundo.es

Estado Mayor Conjunto de las Fuerzas Armadas. (2019). *PC 20-01 Planeamiento para la Acción MiIlitar Conjuta a Nivel Operacional - Proyecto.* Estado Mayor Conjunto de las Fuerzas Armadas.

Fernández, F. A., & González Martín, M. A. (30 de 12 de 2015). *Las generaciones de guerras: Guerras de segunda y tercera generación (II).* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/

Fernández, F. A., & Montesinos. (25 de 11 de 2015). *Las generaciones de guerras: Guerras de primera generación (I).* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/

Fernández, R. (30 de 12 de 2011). *Yulia Timoshenko, trasladada a una cárcel del noroeste de Ucrania.* Obtenido de El País: https://elpais.com/internacional/2011/12/30/actualidad/1325235771_382421.html

Garcia Solórzano, N. I. (2013). La influencia del punto culminante en los conflictos de cuarta generación y su aplicación en el planeamiento operacional. *Trabajo Final Integrador*. CABA, Argentina: Escuela Superior de Guerra Conjunta.

Greenberg, A. (06 de Junio de 2017). *How an Entire Nation Became Russia's Test Lab for Cyberwar.* Obtenido de Wired: https://www.wired.com/story/russian-hackers-attack-ukraine/

Grogovinas, C. A. (2018). La visualización de un marco referencial para el nivel operacional. *Trabajo Final Integrador*. CABA, ARGENTINA: ESCUELA SUPERIOR DE GUERRA CONJUNTA.

Instituto Nacional de Ciberseguridad. (s.f.). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario.* Obtenido de Gobierno de España: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Jaitner, M. (2015). Russian information warfare: Lessons from Ukraine. En K. Geers, *Russian Aggression against Ukraine* (págs. 87-94). Tallin: NATO CCD COE Publications. Obtenido de https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf

Kristiansen, M., & Hoem, N. (14 de Febrero de 2021). *Russian Cyber Strategy*. Obtenido de Small Wars Journal: https://smallwarsjournal.com/jrnl/art/russian-cyber-strategy

Lange-Ionatamishvili, E., & Svetoka, S. (2015). Strategic Communications and Social Media in the Russia Ukraine Conflict. En K. Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (págs. 103-111). Tallin: NATO CCD COE Publications. Obtenido de http://195.222.11.251/uploads/2018/10/Ch12_CyberWarinPerspective_Lange_Svetoka.pdf

Lewis, J. (2015). *Operation Armageddon: Cyber Espionage as a strategic component of Russian modern warfare*. Obtenido de Lookingglass: https://lookingglasscyber.com/blog/threat-intelligence-insights/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/

Lind, W. S. (2005). Comprendiendo las guerras de cuarta generación. *Military Review*, 12-17.

Makotczenko, M. (2019). Una nueva visión de la estratégia militar en la concepción del general de la federación rusa, Valery Gerasimov. *Visión Conjunta*, 20-24.

Martinez Pontijas, J. (11 de Diciembre de 2020). *Control reflexivo: mucho más que desinfomración a la rusa*. Obtenido de Intituto Estratégico: http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO159_2020JUAMAR_controlreflexivo.pdf

Medero, G. S. (2010). Los estados y la ciberguerra. *BOLETIN DE INFORMACIÓN (MINISTERIO DE DEFENSA)*, 63-76.

Pakharenko, G. (2015). Cyber operations at Maidan: A firts-hand account. En K. Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (págs. 59-66). Tallin: NATO CCD COE Publications. Obtenido de https://ccdcoe.org/uploads/2018/10/Ch07_CyberWarinPerspective_Pakharenko.pdf

Pardo de Santayana, J. (09 de Junio de 2021). *¿Porqué a Rusia le interesa tanto Ucrania?* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_analisis/2021/DIEEEA25_2021_JOSPAR_Rusia.pdf

Raychev, Y. (2019). *Cyberwar in Russian and Usa military-political thought: a comparitive view*. Obtenido de Information & Security: https://doi.org/10.11610/isij.4326

Salmón, E., & Rosales, P. (2014). Rusia y la anexión de Crimea o la crisis de post Guerra Fría. *Revista de la Facultad de Derecho*, 185-204.

San Martin, H. (2018). *La guerra híbrida de Rusia sobre Occidente*. New York: Page Publishing Inc.

Sánchez-Vallejo, M. (06 de 04 de 2014). *Activistas prorrusos toman tres edificios gubernamentales en el Este de Ucrania.* Obtenido de El País: https://elpais.com/internacional/2014/04/06/actualidad/1396811045_562024.html

Sepetich, S. E. (2016). Las ciberoperaciones aplicadas a un teatro de operaciones – Estudio de caso: Guerra ruso georgiana. *Trabajo Final Integrador*. CABA, ARGENTINA: ESCUELA DE SUPERIOR DE GUERRA AÉREA.

Shehod, A. (Diciembre de 2016). *Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US.* Obtenido de http://web.mit.edu/smadnick/www/wp/2016-22.pdf

Snegovaya, M. (2015). *Putin´s information warfare in Ukraine.* Washington: Institute for the Study of War. Obtenido de https://www.jstor.org/stable/pdf/resrep07921.1.pdf

Sprang, R. (09 de Noviembre de 2018). *Russia in Ukraine 2013-2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO, and Media.* Obtenido de Small Wars Journal: https://smallwarsjournal.com/jrnl/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and

Trama, G. A. (2017). Operaciones cibernéticas - Su naturaleza, propósito y conducción. *VISIÓN CONJUNTA,* 56-59.

Trama, G. A., & de Vergara, E. (2017). *Operaciones militares cibernéticas - Planeamiento y Ejecución en el Nivel Operacional.* CABA: Visión Conjunta.

Trama, G. A., Guerrero, J. G., & de Vergara, E. (2019). Los ciegos y el elefante: El ambiente operacional híbrido. *Visión Conjunta*, 2-8.

Tsipis, S. (5 de Abril de 2014). *The Ukrainian crisis - a cyber warfare batleffield*. Obtenido de Defense Update: https://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html

Vera Daza, D. (Mayo de 2015). Crisis de Ucrania. *Trabajo Final de Máster*. BARCELONA, España: Universidad de Barcelona.

Vicente, A. L. (2011). La ciberguerra; La guerra inexistente. Madrid, España: Insituto Universotario General Gutiérrez Mellado.

Weedon, J. (2015). Betond cyber war: Russia´s use of strategic cyber espionage and information operations in Ukraine. En K. Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (págs. 67-77). Tallin: NATO CCD COE Publications. Obtenido de https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf