IUE
Instituto de Enseñanza Superior del Ejército
Instituto Universitario Art 77 – Ley 24.521
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "La conducción de las operaciones de ciberdefensa:

Principios básicos en el campo de combate moderno."

Que para acceder al título de Especialista en Conducción Superior de Organizaciones Militares Terrestres, presenta el Mayor Don Luis Javier Anca.

Ciudad Autónoma de Buenos Aires, 18 de agosto de 2015.

Índice de Contenido

Resumen

El presente trabajo analiza el ciberespacio y las acciones que se ejecutan en él, con el fin de determinar los principios básicos que debe aplicar el comandante para la conducción de las operaciones de ciberdefensa.

Con este propósito, se interpreta el ambiente donde se llevan a cabo las operaciones de ciberdefensa y luego, en una segunda parte, se vinculan las operaciones de defensa cibernética en el campo de combate moderno.

El marco referencial teórico considerado es la doctrina básica específica vigente en nuestra fuerza, como así también aquellos documentos legales publicados por el Ministerio de Defensa de la República Argentina, relacionados directamente con la ciberdefensa.

La ciberdefensa en los últimos años se ha posicionado en el mundo como un desafío permanente para aquellas naciones que intentan proteger y conservar su espacio cibernético lo más seguro y confiable posible, aplicando ciertos principios, a fin de lograr la libertad de acción adecuada, buscando un grado de iniciativa tal que permita al comandante conducir las operaciones en el campo de combate.

Palabras clave. Ciberespacio, Ciberdefensa, Principios de ciberdefensa.

Introducción

En los últimos años, al abordar los diferentes ambientes de guerra, la ciberdefensa se ha convertido en un desafío emergente a enfrentar que evoluciona constantemente, haciéndose cada vez más fuerte y preciso en su accionar.

Por tal razón en el campo de combate moderno el comandante deberá ejercer la conducción de su fuerza, teniendo en cuenta este espacio particular denominado ciberespacio.

Hoy, ya no se entiende a los conflictos modernos solo en los espacios tradicionales como tierra, mar y aire, sino que se ha agregado un nuevo ambiente operacional puesto en función con el surgimiento de la nueva "Era de las Tecnologías de la Información". Esta deja atrás los 200 años de la "Era Industrial" y da lugar al desarrollo de una nueva etapa, la de la "Revolución de Asuntos Militares" en el campo de la Defensa Nacional y la Seguridad Internacional, caracterizadas por un avance tecnológico a gran velocidad, que redunda en un nuevo ambiente operacional.

El ciberespacio, se suma al ambiente terrestre y naval, desarrollado desde los orígenes de las civilizaciones y al ámbito aéreo desarrollado en el siglo XX, a partir de la Primera Guerra Mundial y al espacio ultraterrestre surgido durante la denominada Guerra Fría. Emerge así a fines del siglo XX y más categóricamente en este siglo XXI, un nuevo escenario de conflicto. Este se ha convertido en un nuevo dominio, creado por el hombre, en donde ocurren, cada vez con más frecuencia, interacciones. En este sentido, el conflicto armado, como fenómeno social, podría ocurrir y tener injerencia en dicho ambiente.

La evolución de las Tecnologías de la Información y las Comunicaciones (TICs) han provocado un cambio de paradigma que exige la adopción de procedimientos y herramientas especializadas para la neutralización y control de las amenazas cibernéticas, de

todo lo necesario para lograr el provecho propio e impedir su explotación por parte de otros. Varios países, incluyendo los Estados Unidos, han reconocido el ciberespacio como el quinto dominio de la guerra, y están desarrollando formas de operar en los nuevos teatros de operaciones que surgen con él.

La denominada "Guerra Cibernética"[1] es eminentemente asimétrica, ya que es un conflicto violento donde puede existir una gran desproporción entre las fuerzas tanto militares como políticas de los bandos implicados. Por lo tanto obliga a explorar dimensiones históricamente aún no conocidas ni empleadas. Entre estos medios se cuenta con la guerra de guerrillas, toda clase de terrorismo, la contrainsurgencia, el terrorismo de estado y la ciberguerra.

Consecuentemente, los países con fuerzas armadas que más han avanzado en la adopción de sistemas de Comando y Control integrados del tipo Comando, Control, Comunicaciones, Inteligencia, Vigilancia y Reconocimiento (C4ISR), son los que más deben esforzarse en cubrir sus "flancos débiles" derivados del uso intensivo de redes teleinformáticas complejas.

Los hechos sucedidos a nivel mundial fundamentan y justifican el desarrollo de la ciberdefensa como respuesta. Entre los primeros, se pueden mencionar cronológicamente los siguientes ciberataques:

El gusano Morris[2] fue el primer ejemplar de malware[3] autorreplicable que afectó a internet. El 2 de noviembre de 1988, aproximadamente 6000 de los 60000 servidores conectados a la red fueron infectados por este gusano informático, lo que motivó que la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), creara el

[1]Son aquellas acciones de un Estado/Nación, para penetrar las redes y computadoras de otra Nación, con el propósito de causar daño. (Clarke, 2010).

[2]Robert Morris, nacido en 1965. Profesor asociado en el Instituto Tecnológico de Massachussets, en el departamento de Ingeniería Electrónica y Ciencias de la Computación. Es conocido por haber creado el Gusano Morris en 1988.

[3]El malware (del inglés malicious software), código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés) en respuesta a las necesidades expuestas durante el incidente. (Zakon, 1997).

En 2007, Estonia culpó a las autoridades de la Federación Rusa de diversos ataques continuados que afectaron a medios de comunicación, bancos y diversas entidades e instituciones gubernamentales, por medio del DDoS[4]. En ese mismo año el estado de Israel anula los radares antiaéreos sirios mediante un ciberataque, mediante un programa informático desarrollado por Estados Unidos denominado Suter, que permite interceptar las comunicaciones enemigas, infiltrarse en su sistema y llegar a bloquear dichas comunicaciones.

Seguidamente en el 2008, se produce un ataque a Georgia y en el 2009 del mismo modo a Corea del Sur. Durante el año 2010 una central nuclear de Irán fue atacada por Stuxnet, un gusano informático que afecta a equipos con Windows.

Años más tarde, en el 2011, surge la aparición de una serie de gusanos informáticos capaces de realizar ataques cibernéticos, tales como Conficker, Ghostnet, Night Dragon, Aurora, Anonymous, Antisec, Shady Rat, etc.

Al año siguiente, por medio de un virus iraní, son formateados 30 mil ordenadores de Saudi Arabian Oil Co. Finalmente y como hechos más recientes han ocurrido en el 2013 los siguientes episodios: Ciberataques sirios contra sitios web de prensa norteamericana; Corea del Norte atacó a sistemas de Corea del Sur y los Estados Unidos; China robó secretos industriales de contratistas de defensa de EEUU NSA PRISM[5].

En lo que respecta a los Estados Unidos el 21 de mayo de 2010 anuncia la creación del primer cibercomando conjunto a nivel mundial (U.S. Cyber Command – USCYBERCOM) bajo el mando del comando estratégico militar. Su objetivo fue a integrar

[4]El objetivo de un ataque DDoS (Distributed Denial of Service) es inhabilitar un servidor, un servicio o una infraestructura sobrecargando el ancho de banda del servidor o acaparando sus recursos hasta agotarlos.

[5]Es un programa de vigilancia electrónica considerado confidencial a cargo de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos desde el 2007.

mancomunadamente los esfuerzos y capacidades de los cibercomandos de cada una de las fuerzas armadas de ese país. A continuación en 2011, surge el denominado Ciber Ejército Azul de la República Popular China, mientras que a principios del 2012 se manifiestan actividades militares de la Federación Rusa en el ciberespacio, conforme a lo publicado por el Ministerio de Defensa de dicho país. Por otra parte, el Reino Unido de Gran Bretaña, cuenta actualmente con el Programa Nacional de Seguridad Cibernética, tendiente a ampliar los sistemas de protección de la seguridad en ese campo. (Ortiz, 2012).

Por su parte, la República Federal de Alemania ha explicitado sus capacidades de ciberdefensa en un informe oficial en el cual se considera que, a la luz de los ataques realizados contra redes gubernamentales durante los últimos años, el país debe ponerse al nivel de los otros que integran la Organización del Tratado del Atlántico Norte (OTAN). Esta sucesión de ataques y necesidades de protección, a través de la creación de comandos de ciberdefensa, ha exigido a los países de América del Sur tratar de colocarse a un mismo nivel que el resto del mundo, como Brasil, donde el Ministerio de Defensa creó en el ámbito del Ejército al Centro de Defensa Cibernético. (Ortiz, 2012).

Estos hechos evidencian que, las agresiones entre estados naciones y actores estratégicos no estatales utilizando malware sumamente sofisticado, ha causado en algunos casos efectos devastadores, como se ha venido verificando, con especial intensidad, desde el año 2007. En este mismo contexto, la región de Sudamérica no ha permanecido ajena a estos actos hostiles.

En lo que respecta a la República Argentina, la Ley 23.554 (1988) define a la Defensa Nacional como la integración y la acción coordinada de todas las fuerzas de la nación para la solución de aquellos conflictos que requieren el empleo de las fuerzas armadas, en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por

finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes.

Por ello, el Ministerio de Defensa de la República Argentina, publicó la actualización del Libro Blanco de la Defensa (2010), donde en materia de ciberdefensa se expone:

> Considerar estratégico avanzar en la investigación, desarrollo y aplicación de las tecnologías aeroespaciales, nucleares y aquellas vinculadas al ciberespacio desde el Sistema de Defensa Nacional, en el marco de lo establecido en la Constitución Nacional y los múltiples acuerdos vigentes.
>
> Las tecnologías aeroespaciales y ciberespaciales constituyen contribuciones críticas para hacer viables los efectos pretendidos en el marco de una estrategia de carácter defensivo. Estas son consideradas esenciales para contar con una alerta estratégica temprana frente a una eventual agresión militar estatal externa, y para desarrollar eficazmente la conducción de las operaciones militares y repeler con éxito dicha agresión. (p48)

A tal efecto, el Ministro de Defensa (2014) dictó la Resolución MINDEF 343 del 14 de mayo de 2014, con la finalidad de crear el Comando Conjunto de Ciberdefensa. Su misión es elaborar el Plan de Empleo de la Ciberdefensa e instruir a los Estados Mayores Generales (EMG) de las Fuerzas Armadas como disponer medidas pertinentes para la seguridad de la información.

De este modo, la Directiva de Política de Defensa Nacional (DPDN), 2645/14 del Ministerio de Defensa de la República Argentina (2015), manifiesta la asociación de nuevos paradigmas tecnológicos y a las tecnologías de la información al denominado ciberespacio para el desarrollo de operaciones militares.

En lo que respecta al ciberespacio y su uso en la defensa, su dominio no sólo resulta esencial para el ejercicio del comando y control, y para el funcionamiento en red del sistema, sino también para repeler amenazas militares, como así también otros actores estratégicos que puedan producirse utilizando al llamado ciberespacio como vía de ejecución o teniéndolo como objetivo.

En el ámbito de la Escuela Superior de Guerra se han realizado trabajos y artículos abordando aspectos referidos al ciberespacio y otros referidos a la revolución de asuntos militares y las nuevas tecnologías. Algunos de estos trabajos han sido considerados en este estudio, Guerra Cibernética (Stel, 2005), da un primer marco teórico para el inicio del presente trabajo, como así también el trabajo final de sobre La evolución del Ejército Argentino en seguridad informática, en el marco de operaciones militares llevadas a cabo en el ciberespacio (Palacio, 2013).

También se ha tomado en cuenta para este trabajo el pensamiento del Coronel García perteneciente al Comando Conjunto de Ciberdefensa de las Fuerzas Armadas Argentinas, con quien se mantuvo una entrevista.

Además se realizó una consulta personal, con el Centro de Defensa Cibernética de la República Federativa del Brasil, en relación con los temas de organización y principales pilares en materia de ciberdefensa en dicho país.

El diseño metodológico hace de este trabajo una investigación bibliográfica de carácter descriptivo, con análisis documental de fuentes primarias y secundarias, como documentos disponibles en línea, páginas web, periódicos, reglamentos y manuales vigentes.

El presente trabajo incluye, en el primer capítulo algunas consideraciones sobre el nuevo ambiente operacional, el cambo de combate moderno y el ciberespacio, las características del ciberespacio y la ciberdefensa en la República Federativa del Brasil. El

segundo capítulo se centra la atención en la defensa cibernética, las operaciones de ciberdefensa, la conducción en las operaciones de ciberdefensa.

Se quiere expresar, en lo que respecta al aporte sobre el pensamiento militar y como fundamento contribuyente a la conducción superior de organizaciones militares terrestres, que debido a lo citado anteriormente y de la información disponible, como así también los acontecimientos recientes en el mundo, se evidencia la necesidad de insertarse en esta problemática en el concepto de ciberdefensa, como nueva dimensión y ámbito o escenario de la guerras del siglo actual, en donde se ejecutarán acciones cibernéticas y en el cual el comandante buscará optimizar su empleo en forma efectiva para enfrentar agresiones que provengan de él, como así también la de asegurar y proteger el propio espacio, logrando con esto soberanía sobre el ciberespacio e incremento de capacidades que hacen a la Defensa Nacional.

El marco referencial, en donde se encuadra este trabajo se basa en la doctrina básica específica y conjunta vigente en nuestra fuerza, como así también en documentos legales publicados por el Ministerio de Defensa de la Argentina, relacionados directamente con la ciberdefensa.

Lo mencionado anteriormente está en función de los aspectos legales que rigen en el país, ya sea la ley de Defensa Nacional Nro 23554, la Resolución MINDEF 343 / 14MAY14, la ley de Restructuración de las FFAA Nro 24948. Como así también, se tendrá consideración aquellas materias particulares relacionadas con la Especialización en Conducción Superior de Organizaciones Militares Terrestres, logrando la integración entre ellas a fin de dar cumplimiento a la finalidad buscada.

Se considera que la composición heterogénea del espacio cibernético, que requiere la emergencia de un nuevo campo de combate y la elevada complejidad que supone el análisis de los casos de intervención, implican la posibilidad de una participación dire-

cta de muchas más disciplinas de las que podría abarcar cualquier investigador. Por lo tanto, cabe aclarar que, el recorte necesario que limita al presente estudio, no es a los fines de simplificar la mirada sobre el objeto, sino condición de posibilidad para volverlo afable. El estudio estará limitado al campo disciplinar militar, específicamente al nivel táctico y sin involucrar aspectos técnicos tecnológicos.

El Componente Terrestre aún no se encuentra preparado para hacer frente a este tipo de amenaza, que además extiende su agresión informática ilimitada en tiempo y espacio. En aquel espacio cibernético, definido como un nuevo ámbito para efectuar operaciones militares, plantea un sinnúmero de interrogantes. Entonces, ¿Cuáles deberán ser los principios básicos que rigen la conducción de las operaciones de ciberdefensa?

Para dar respuesta a este interrogante y dado el carácter de la ciberguerra los objetivos planteados son:

Objetivo general. Analizar el ciberespacio y las acciones que se ejecutan en él, a fin de determinar los principios básicos que debe aplicar el comandante para la conducción de las operaciones de ciberdefensa.

Objetivos específicos.

1. Interpretar el ambiente donde se llevan a cabo las operaciones de ciberdefensa.
2. Vincular las operaciones de ciberdefensa en el campo de combate moderno.

El ciberespacio

El presente capítulo tiene como propósito interpretar el espacio donde se llevan a cabo las acciones cibernéticas, al cual se lo denomina ciberespacio. Aunque se lo reconoce como un espacio virtual, dado que lo que sucede en él tiene implicancia en el ambiente físico, se lo considera parte integrante del factor de espacio.

Kuehl (2009) al definir el término, afirma que es el dominio operacional cuyo carácter distintivo y único está enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar la información, a través de los sistemas basados en las Tecnologías de Información y Comunicaciones (TICs) y también sus infraestructuras asociadas.

En el concepto de Kuehl se aprecia una vinculación entre el espectro electromagnético y las redes informáticas, aunque no deben confundirse estos dos términos ya que la Guerra Electrónica se corresponde con los ámbitos tradicionales de los conflictos: Tierra, Mar y Aire, mientras que la Guerra Cibernética se desarrolla entre dos o más actores, en un nuevo ámbito de las hostilidades: el ciberespacio.

En la Argentina, la Directiva de Política de Defensa Nacional (DPDN), Decreto 2645/14 del Ministerio de Defensa (2015), afirma que la dimensión ciberespacial, sin localización física y concreta, genera replanteos en función de la guerra real y exige por la dinámica de la tecnología, una rápida adaptación de los sistemas de defensa.

En este sentido se considera el ciberespacio como un campo de combate igual a la tierra, el mar, el aire o el espacio y, por tanto, sujeto a ataques preventivos y represalias.

En el Reglamento de Conducción para las Fuerzas Terrestres (Ejército Argentino, 2015), se menciona que la conducción táctica constituye el nivel de ejecución por excelencia e involucra el concepto de fuerza aplicada. Lleva implícita la lucha de voluntades

entre dos o más enemigos, y consiste en la búsqueda permanente de la libertad de acción que permita alcanzar los propios objetivos.

Se puede señalar que el nivel de conducción táctico es el arte de conducir los medios del poder de combate en un delimitado espacio y en un determinado lapso para lograr el efecto deseado por el nivel operacional. De esta manera se establece que la táctica posee tres factores bien definidos que son el espacio, el tiempo y el poder de combate relativo.

Ahora bien, se entiende al ciberespacio como parte del espacio, siendo éste junto, con el tiempo y las fuerzas, uno de los denominados factores de la táctica. O sea, factores que condicionan al comandante en la consecución de sus objetivos. Estos mismos son constantes y proporcionan el marco referencial para la ejecución de las operaciones.

Según el Reglamento de Conducción para las Fuerzas Terrestres (Ejército Argentino, 2015), el espacio, el tiempo y el poder de combate relativo tendrán una relación e influencia recíproca y proporcional entre ellos, teniendo en cuenta que el espacio es el factor que delimita en forma tridimensional la ejecución de acciones a llevar a cabo por las fuerzas. Siendo estas aquellas que en un tiempo determinado deberán actuar para enfrentar acciones cibernéticas, tanto pasivas como activas.

El ciberespacio, se define, también, como un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas. (Lorents, 2010). Lo expresado señala, claramente al factor espacio como ciberespacio, en función de un tiempo determinado, siendo los sistemas que actúan y los usuarios, las fuerzas enfrentadas.

Aceptando las distintas definiciones del ciberespacio, se lo interpreta como un nuevo espacio descubierto por el hombre, que no es solo virtual sino que lo sucedido en él tendrá implicancias en el espacio físico, en el cual se desarrollan actividades cuyo fin es

proteger y dislocar el ciberespacio del adversario si fuese necesario, considerando a estas acciones como un factor más influyente en el ambiente operacional.

Por ello, el Ambiente Operacional Futuro es considerado por el Reglamento de Doctrina Básica para la Acción Militar Conjunta (EMCO, 2014) como la participación de las Fuerzas Armadas en futuros conflictos interestatales que estará marcada por la dimensión dual autónoma, cooperativa de la Defensa Nacional. En tal sentido, la conducción de las fuerzas puestas a disposición del Comandante Operacional durante la campaña se verá influenciada por la amplia naturaleza de los efectos a lograr, los estados finales a alcanzar y los riesgos asociados, por lo que su cabal comprensión en términos operacionales resultará gravitante para alcanzar el éxito deseado.

En una aproximación al análisis sistémico, los factores componentes del ambiente operacional se aplican a todos los niveles de conducción y ámbitos específicos de cada fuerza, los mismos afectan el desarrollo de toda la campaña. Es prácticamente imposible hacer distinciones para su análisis y posteriores conclusiones en los diferente ámbitos de competencia (terrestre, aéreo o naval). Los estudios para la determinación de las características del ambiente operacional deberán ser elaborados en los diferentes niveles de la conducción, su progresión metodológica deberá ser concurrente con el planeamiento al cual interesa y servirá como antecedente a los escalones inferiores quienes incrementarán los detalles pertinentes a sus necesidades específicas.

El modo de abordar los factores no puede ser aislado, sino que tienen que verse como parte de un todo. No es la suma de elementos, sino un conjunto de elementos que se encuentran en interacción, de forma integral, que produce nuevas cualidades con características diferentes, cuyo resultado es superior al de los componentes que lo forman.

Los factores disponen entre sí relaciones interdependientes compleja y multidisciplinaria, por lo tanto la importancia no radica en la identificación del tipo de factor que se

trata, sino en la interrelación que tiene con los demás. Vale decir que todas aquellas actividades que suceden en el ciberespacio guardan una relación no solo entre ellas sino también con otros factores del ambiente operacional, que el comandante deberá estar en capacidad de afrontar a fin de conducir las operaciones en el campo de combate moderno en forma eficiente.

La Revolución de Asuntos Militares como compendio aclarador de las características que enmarcan al poder militar debe satisfacer las necesidades que se le asignan a los factores del ambiente operacional. Es por esto que es necesario complementar los factores del componente terrestre con el nuevo espacio operacional, para formar un escenario más claro donde se ejecutará el combate moderno.

Como fundamento de la necesidad de complementación se entiende que los conflictos armados adquieren características propias de la situación y circunstancia que los rodea. Como así también, que en la actualidad el ambiente operacional requiere la utilización de métodos de análisis sistémicos.

La revolución de asuntos militares y, en particular, el exponencial crecimiento de la tecnología y la necesidad de la información, implícita en la idiosincrasia del hombre, exigen realizar cambios en la doctrina vigente.

Considerar al espacio cibernético como un entorno operativo tales como tierra, mar, aire y espacial, como parte integrante del ambiente operacional en donde se desarrollan acciones militares y su influencia en la conducción será de relevancia para el comandante.

El ámbito terrestre del campo de combate y del ciberespacio

El ámbito terrestre del campo de combate, por sus características propias y distintivas, está expuesto a situaciones complejas marcadas por la interacción e influencias mutuas entre los diversos actores que en él se encuentran, los constantes cambios en la

situación general, acompañados por el avance y el desarrollo de las tecnologías y su incidencia directa en las formas de relacionarse de las sociedades. Es por este motivo que para analizar y extraer características distintivas del ambiente terrestre, el comandante deberá comprender profundamente el ambiente en el cual desarrolla sus operaciones y la forma en que éstas influyen, de manera de estar en condiciones de poder apreciar los posibles efectos tanto favorables como adversos, que sus acciones generen.

Los avances tecnológicos presentan oportunidades y desafíos para el desarrollo de las capacidades operacionales de las fuerzas terrestres. Las capacidades de los hombres desde el conocimiento y el adiestramiento que la fuerza puede dar en el uso de la tecnología disponible, serán factores que se deberán considerar para establecer las capacidades reales de una organización.

Por otra parte, la aceleración de los tiempos, se verá reflejada en los menores tiempos para las alertas, el alistamiento y la respuesta a la agresión. Como así también el incremento del alcance operacional, influido por los sistemas de armas, de vigilancia y de comunicaciones y la necesidad de operar en regiones distantes.

Dado que las Fuerzas Armadas son, cada vez más, dependientes de los recursos digitales y las redes informáticas, está emergiendo un campo de batalla cibernético. Como la tecnología que permite la comunicación y procesado de la información cambia tan rápidamente, las Fuerzas Armadas debe evaluar continuamente qué aptitudes y capacidades son las necesarias para conseguir, conservar y explotar las ventajas en este emergente campo de combate moderno. El modo en el que las tecnologías del ciberespacio se integran y emplean, según las circunstancias operativas de cada momento, afectará significativamente al desarrollo y resultado de las operaciones militares.

Dentro de las características del campo de combate actual, aparecen las operaciones continuas, producto de los avances tecnológicos que las han hecho posibles. Sin embar-

go, las operaciones continuas o de alto ritmo imponen una gran exigencia en los sistemas relacionados con el sostén logístico y pone a prueba severamente la resistencia de los soldados y del equipamiento. El adiestramiento de la fuerza debe contemplar la preparación para la ejecución de operaciones continuas, ello se logrará, a través de cambios organizacionales, el adiestramiento operacional y la explotación de la tecnología disponible. (Ejército Argentino, 2015)

Se puede considerar que dentro del ciberespacio se ejecutan las operaciones de configuración de la ciberdefensa, las que se llevan a cabo, en cualquier nivel, que crearán o preservarán las condiciones favorables para el éxito de la operación decisiva. Por lo general logrará accionando sobre las variables del enemigo, del terreno y la relación con la población local. Las operaciones de configuración podrán ejecutarse antes, durante y después de las operaciones decisivas. Se deberán tener presente que las operaciones de configuración deberán ser concebidas sobre la base de las necesidades de la operación decisiva, para quien crea o mantiene las condiciones favorables.

Para ello, los sistemas y arquitecturas de redes informáticas deben contar con una elevada interconexión, donde el empleo de comunicaciones centradas en redes incremente la interoperabilidad y trae aparejado una mejora en el acceso a la información, desde una gran variedad de fuentes. Esto sirve para aumentar el flujo de la información entre el campo de batalla y el mundo exterior, agregando un nuevo nivel de complejidad a los comandantes de las distintas organizaciones.

Las comunicaciones más eficientes también posibilitan a los comandantes adoptar mejores resoluciones y así permitir que fuerzas dispersas y más pequeñas puedan lograr mayores efectos en el combate. La creciente interconexión brinda la posibilidad cierta de establecer una arquitectura de comunicaciones que pueda enlazar todos los sistemas

operativos de combate hasta los menores niveles, para hacer posible el logro de efectos en el combate en sintonía con la intención del comandante.

Considerando al Reglamento de Conducción para las Fuerzas Terrestres (2015) se denomina ámbito terrestre como aquel que comprende la superficie terrestre, incluidas las áreas fluviales y lacustres interiores, las zonas marítimas adyacentes y el espacio aéreo necesario para el empleo de los medios terrestres, como así también, al espectro electromagnético y al ciberespacio.

Desde esta perspectiva, el ciberespacio es parte sustancial del ámbito terrestre, dentro del cual el comandante deberá accionar a fin de lograr un espacio seguro que permita la obtención de la libertad de acción para el desarrollo de las operaciones, ya que toda acción enemiga en el ciberespacio podría alterar y paralizar al comando y al control propio.

El ciberespacio como un nuevo escenario de combate

Para el Diccionario de la Real Academia Española (2012) un escenario es un lugar donde ocurre o se desarrolla un suceso. Por otra parte, un escenario de conflicto es el lugar donde ocurre o se desarrolla un conflicto. La Historia revela que a lo largo de los siglos, el ser humano ha ido extendiendo sus zonas de conflicto a aquellos escenarios que progresivamente ha ido dominando, ya sea del tipo natural y artificial.

Los escenarios físicos son los llamados escenarios tradicionales de conflicto, los que están delimitados por un entorno físico, natural o artificial, con dimensiones y fronteras, ocupando extensión o espacio y que pueden ser determinados y definidos mediante la utilización de aparatos de medida.

El instrumento de poder militar, para poder ejercer su fuerza sobre los escenarios, requerirá disponer de unas capacidades militares defensivas y ofensivas y unos medios que permitan alcanzar la superioridad en cada entorno militar específico.

De acuerdo con lo expresado anteriormente, se puede afirmar que es en este ambiente donde se llevarán a cabo las operaciones de ciberdefensa. Es por consiguiente, un nuevo espacio en el que se desarrollarán los conflictos modernos.

La Revolución de Asuntos Militares (RAM) se basa en nuevas tecnologías y cambios en las estructuras organizativas, incorporando conceptos operacionales innovadores que incrementan el potencial militar considerablemente. Las implicancias de la RAM, tienen un alto impacto sobre las operaciones militares. Esto implica cambios en la conducción de la guerra. Uno de ellos, el que las fuerzas dependen cada vez más del flujo de información necesaria para el sistema operativo de cada armamento particular, por lo tanto, la "Guerra de la Información" ha transformado al espacio actual en un conflicto de cuatro dimensiones.

El hombre vive en un estado de conflicto permanente por naturaleza y para resolver sus diferencias de intereses utiliza los instrumentos del poder que tiene a su disposición. Es así como el poder militar actúa sobre el entorno físico, para cuyos escenarios las naciones han formado y capacitado sus ejércitos profesionales.

Los escenarios tradicionales de conflictos, están delimitados por un entorno físico, natural o artificial con dimensiones y fronteras, que son determinados y medibles. Sin embargo, es en este punto donde se debe tener en cuenta la existencia de un nuevo escenario donde se desarrollan los conflictos modernos, denominado ciberespacio.

Si sólo se define el ciberespacio a través de una definición virtual, ficticia, o metafórica se presentarían dos problemas claves. En primer lugar, sería difícil construir capacidades militares reales o conductas militares reales en un dominio que no existe realmente en forma tangible. En segundo lugar, esta definición no podría explicar en forma medible, los eventos de la guerra real que suceden en el ciberespacio y producen impactos en cada sistema informático, en identidades robadas, vidas, tiempo, trabajo, datos

destruidos o comprometidos e impactos monetarios asociados, en cortes de la red eléctrica, en los vuelos de las aerolíneas con retraso, produciendo efectos tanto positivos como negativos en el mundo físico. Las señales bits y bytes son fenómenos reales mensurables, por lo tanto, el ciberespacio no es ni una metáfora, ni un mundo virtual, y ficticio del medio ambiente, ni una alucinación. El ciberespacio es real y debe ser definido en términos reales. (Cloud, 2007).

Es aquí que interpretando a Cloud (2007), se pude decir que en su opinión entiende al ciberespacio como un espacio real, mientras otros autores lo interpretan como un espacio virtual con implicancias en el ambiente físico.

En la Argentina, el Libro Blanco de la Defensa, (Ministerio de Defensa, 2010) define al ciberespacio como:

> Las tecnologías destinadas a asegurar la confidencialidad, integridad y disponibilidad de la información esencial para mantener la continuidad operativa del ciberespacio que configura una nueva dimensión operacional –independiente y omnipresente– en los espacios terrestres, marítimos y aeroespaciales de jurisdicción e interés. Desarrollo de ingenios militares, capacidades, organizaciones y recursos humanos que aseguren el uso y el control del ciberespacio específico de los componentes del Sistemas de Defensa Nacional, y aquellos ámbitos de interés estratégico asociados ante agresiones externas contra el ciberespacio nacional. (p278)

Por otra parte, siguiendo a Palacios (2012) se puede interpretar al ciberespacio como:

> Las tecnologías de la información han tenido una distribución rápida y generalizada desde su nacimiento. Se puede decir que en la actualidad se emplean a nivel mundial para la gestión de casi cualquier actividad. Esto, que a priori prometía ser de una utilidad extrema, por lo que a términos de eficiencia se refiere, ha creado a su vez nuevas amenazas a la discreción y seguridad, al recaer la casi totalidad del pa-

trimonio o control de los procesos de una organización en dichos sistemas. (Palacio J, 2012, p6)

Considerando estos dos últimos conceptos, se los puede vincular con un denominador común, tal como un escenario de interés el que deberá ser protegido, mediante acciones que logren hacerlo seguro y confiable de manera de utilizar los medios tecnológicos y proporcionar seguridad a las infraestructuras críticas a fin de contribuir a la defensa nacional.

Dentro del espacio cibernético, existen infraestructuras críticas, que de algún modo deben ser protegidas ante aquellas amenazas que desestabilicen la situación normal, de la cual dependen los servicios básicos y los sistemas de producción de cualquier sociedad. En tal sentido, una interrupción ocasionada por una acción cibernética, tendría graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad. (Bejarano, 2011).

Por consiguiente, el ciberespacio es el dominio global y dinámico compuesto por infraestructuras de tecnología de la información, incluyendo internet, redes de telecomunicaciones y sistemas de información.

El relativamente reciente proceso de digitalización que incorporó sistemas y redes basadas en tecnologías de la comunicación e informáticas, en todos los ámbitos de la sociedad y del Estado, se agregó al nuevo ambiente operacional conocido el ciberespacio o espacio cibernético. Este dominio, en el que no existen fronteras y en el que los niveles de la guerra no pueden identificarse, aunque estas fronteras sean determinantes a la hora de establecer los bienes a proteger, porque las características de las acciones durante la crisis y conflictos que en este se desarrollen, influyen de manera decisiva en relación con las acciones de respuesta que se planteen.

De esta manera, cada una de las arquitecturas informáticas que se sitúan geográfica y físicamente en un entorno determinado, sirviendo a través de unas determinadas identidades a personas concretas, constituyen un complejo ámbito de actuación donde se desarrollan los cometidos específicos de la ciberdefensa.

La aproximación a este entorno que constituye el ciberespacio de interés, se debe situar como un espacio minúsculo dentro de la extraordinaria complejidad que constituye este ámbito global.

Es en este nuevo dominio, el ciberespacio, es donde deberán realizarse considerables esfuerzos los próximos años para dotar a las Fuerzas Armadas de las capacidades necesarias para garantizar su libertad de acción en las operaciones militares que se desarrollen o apoyen en él, teniendo en cuenta que no constituye un espacio en sí mismo, sino una dimensión que atraviesa los límites con reglas y medios propios.

Al respecto, consultado el Coronel García del Comando Conjunto de Ciberdefensa, ha señalado que el ciberespacio es un ámbito virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de información y comunicaciones. Constituye un ámbito de actuación operacional de cualquiera de las Fuerzas Armadas y otros actores cibernéticos. (Comando Conjunto de Ciberdefensa, comunicación personal, febrero de 2015).

Concluye García que el comandante deberá lograr un ciberespacio seguro y confiable, teniendo en cuenta que el mismo evoluciona continuamente, a fin de contar con una adecuada libertad de acción, evitando en todo momento los riesgos derivados del ciberespacio, que podrán llegar a afectar el equilibrio del sistema, provocando la dislocación del mismo.

La importancia de un ciberespacio seguro

Por lo dicho hasta el momento, se puede establecer que la necesidad primordial del comandante es lograr un mayor control del espacio cibernético para que devenga en un ámbito seguro, y tienda a mantenerse como un ambiente desregulado y libre del control enemigo. En definitiva, el problema discurre entre la necesidad de proteger las redes y los servicios de información, y a su vez, las infraestructuras críticas, redes logísticas, como aquellas redes digitales que posibiliten el comando y el control de la operación.

Por otra parte, Touré (2011) integrante de la Unión Internacional de Telecomunicaciones (UIT), expresa que las tecnologías de la información y la comunicación (TICs) se han convertido en parte del nuevo escenario y tienen influencia en el desarrollo de las operaciones militares. Las comunicaciones, las redes y los sistemas digitales proporcionan a la comunidad mundial los recursos esenciales y la infraestructura indispensable, para lograr una estabilidad sin la cual las fuerzas terrestres podrían entrar en una situación de crisis.

Así es como estas estructuras podrían quedar expuestas a ataques de una diversidad ilimitada y sin precedentes, considerando además, que este tipo de ataques se podrían producir sin previo aviso y en forma sorpresiva.

En el campo de combate moderno, en una situación así, todo quedaría fuera de servicio, las redes de computadoras, la telefonía celular, los sistemas de control del tráfico terrestre, naval y aéreo. La caída de la red eléctrica dejaría en la oscuridad más absoluta a los hospitales y los hogares. Las autoridades gubernamentales serían incapaces de evaluar los daños, comunicarse con el resto del mundo para informar sobre la crisis o proteger a sus vulnerables ciudadanos contra los subsiguientes ataques. Lo descripto llevaría a un país, a una situación crítica, paralizando a sus gobernantes, impidiendo que tomaran decisiones eficientes y rápidas.

Touré (2011), afirma que el ciberespacio es un ámbito virtual y conceptual en el que existen dos sistemas, un componente humano y uno tecnológico. Por consiguiente, el significado general de "guerra cibernética" es el de una guerra que se lucha en el ciberespacio y donde las TICs son a su vez las armas y los objetivos y todo ello en función al tiempo determinado.

Las Fuerzas Armadas tienen una alta dependencia de las Tecnologías de la Información y las Comunicaciones (TICs), ya que estas constituyen un pilar básico para poder llevar a cabo las operaciones militares. Sin embargo, este nuevo dominio donde operan estas tecnologías y que se ha denominado ciberespacio, está lleno de un gran número de amenazas que ponen en peligro el éxito de las operaciones militares, así como también a las personas que las llevan a cabo.

Tradicionalmente, la seguridad en las TICs en el ámbito militar se ha centrado en la protección de las comunicaciones, aunque hoy en día el uso masivo de sistemas de información hace necesario disponer de una perspectiva más amplia y abordar el problema de una forma integral.

El ciberespacio en Brasil y la situación en Argentina

Es importante destacar que lo expuesto no pretende de forma alguna importar criterios, facilidades y/o doctrina que poco se ajustarán a las particulares necesidades, pero cierto es que se debe tener en cuenta la notable ventaja de explotar las experiencias obtenidas por otros.

Se cree necesario en este punto explicar el porqué de la elección de este país para establecer un modelo. Brasil, obedece a un país del ámbito regional, con las mismas características que la República Argentina y con él quien se está trabajando en forma mancomunada.

Se aclara que no se pretende dar aquí un catálogo de especificaciones técnicas del material utilizado por los diferentes sistemas, por el contrario la problemática se abordará desde lo conceptual, destacando todos aquellos aspectos que tipifiquen y distingan las características que permitan obtener conclusiones válidas.

El ciberespacio en Brasil. Este país enmarca sus políticas de ciberdefensa en función al Libro Estrategia de la Defensa Nacional (2008) del Brasil, en el cual se menciona la acción de estimular la integración de América del Sur, en donde expresa:

> Esa integración no solamente contribuirá para la defensa de Brasil, como posibilitará fomentar la cooperación militar regional y la integración de las bases industriales de defensa. Alejará la sombra de conflictos dentro de la región. Con todos los países se avanza rumbo a la construcción de la unidad de América del Sur. El Consejo de Defensa de América del Sur, en discusión en la región, creará mecanismo consultivo que permitirá prevenir conflictos y fomentar la cooperación militar regional y la integración de las bases industriales de defensa, sin que de ello participe país ajeno a la región. (p17)
>
> Las capacitaciones cibernéticas se destinarán a la más amplia gama de usos industriales, educativos y militares. Incluirán, como parte prioritaria, las tecnologías de comunicación entre todos los contingentes de las Fuerzas Armadas de modo a asegurar su capacidad para actuar en red. Contemplarán el poder de comunicación entre los contingentes de las Fuerzas Armadas y los vehículos espaciales. En el sector de la cibernética, será constituida una organización encargada de desarrollar la capacitación cibernética en los campos industrial y militar. (p33)
>
> El Ministerio de Defensa y las Fuerzas Armadas intensificarán las coparticipaciones estratégicas en las áreas cibernética, espacial y energía nuclear y el intercambio militar con las Fuerzas Armadas de las naciones amigas, en este caso

particularmente con las del entorno estratégico brasileño y las de la Comunidad de Países de Lengua Portuguesa. (p33)

Organización. En Brasil la organización se inicia en Estado Mayor Especial (EME), entre otras funciones, se encarga de la planificación, dirección, coordinación y evaluación a nivel de dirección general, las actividades relacionadas con los Sistemas de Inteligencia, Información Organizacional, Medios, Comunicaciones, Computadoras, Guerra Electrónica, Fotos, las Operaciones Psicológicas y de Información Operacional. Por consiguiente, del EME también se toman las tareas relacionadas al despliegue del Sector Cibernético.

Sin embargo, las organizaciones militares directamente relacionados con el Sector de Ciberdefensa del Ejército de Brasil son en su mayoría subordinadas al Departamento de Ciencia y Tecnología (DCT). El DCT, comprende la Información del Grupo de Seguridad, responsable de llevar a cabo la investigación científica, el desarrollo experimental, el asesoramiento científico y técnico, la aplicación de conocimientos y dominar las tecnologías de seguridad de la información.

Otra organización militar que también tiene relación con el sector cibernético es el Centro de Inteligencia del Ejército (CIE), un órgano consultivo que depende directamente del Comandante del Ejército, cuya misión es contribuir al proceso de toma de decisiones y la producción de la Inteligencia para el cumplimiento misión del Ejército. La CIE también tiene en su estructura organizativa la Escuela del Ejército de inteligencia militar (EsIMEx), que apoya cursos de inteligencia de señales y la ciberguerra, además de la realización de cursos de información geográfica del ejército. (Carneiro, 2012).

Pilares básico de la política de ciberdefensa. Consultado el Centro de Defensa Cibernética del Brasil, expresa que la eficacia de las medidas de Ciberdefensa depende de

manera fundamental de las actividades de colaboración de la sociedad brasileña, incluyendo no solo al Ministerio de Defensa, sino también a la comunidad académica, sectores público y privado y la base industrial de defensa.

La capacidad tecnológica del sector cibernético debe llevarse a cabo en armonía con la política de la ciencia, Tecnología e Innovación para la Defensa Nacional.

La seguridad de la información y comunicaciones es la base de la Defensa Cibernética y depende directamente de las acciones individuales.

Principales características de la ciberdefensa en Brasil. La ciberdefensa debe ser sencilla, para ello deberá:

Ser dependiente del trabajo conjunto de las Organizaciones Militares con los Órganos Públicos y Privados para que efectivicen la actuación colaborativa.

El desarrollo de nuevas capacidades en las Fuerzas Armadas, en el ambiente empresarial, en el sector público y en la comunidad académica es el principal pilar del sector cibernético.

Entre los principales productos para el Ejército, para el Ministerio de Defensa y para la Nación, se encuentra el desarrollo de la Doctrina Militar de Defensa Cibernética, como el empleo de productos de uso dual, militar y civil.

La situación en la Argentina. Al considerar lo expresado y realizando un breve análisis se puede obtener una comparación en relación a la situación actual en la República Argentina, para ello se tiene en cuenta la organización y algunas características particulares en materia de ciberdefensa.

A partir de la aprobación de la Resolución MD Nº 343/2014, el Instrumento Militar del Sistema de Defensa Nacional comienza a ser incluido en el armado de una estrategia de ciberdefensa. Con ella se crea el Comando Conjunto de Ciberdefensa, dependiente del Estado Mayor Conjunto de las Fuerzas Armadas. Dicha Resolución establece como

misión de éste ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional.

Estas medidas son acompañadas también por el compromiso de la República Argentina por articular políticas de defensa cibernética con otros países del ámbito de la Unión de Naciones Suramericanas (UNASUR). Tales acciones confluyen positivamente en el objetivo de la política de defensa argentina de avanzar progresivamente hacia el logro de un sistema de defensa subregional.

Efectivamente, el 13 de septiembre de 2013 se suscribió en Buenos Aires, una declaración conjunta entre el Ministro de Defensa argentino, Agustín Rossi, y su homólogo del Brasil, Celso Amorim, a través de la cual decidieron impulsar la cooperación en ciberdefensa y la creación de un grupo de trabajo bilateral, el cual se reunió dos meses después en Brasilia y acordó una agenda de trabajo, orientada a las áreas de capacitación, métodos y sistemas tecnológicos, desarrollo de doctrina combinada, investigación científica e intercambios entre los CSIRT (Computer Security Incident Response Team) de ambos ministerios para incrementar la seguridad cibernética. (Escuela de Defensa Nacional, 2014).

En lo que respecta al Ejército Argentino la Dirección General de Inteligencia cuenta con el Centro de Ciberdefensa, creada en noviembre de 2014.

Conformado por un equipo con capacidad de entender la nueva situación de la ciberdefensa y asegurar los eslabones de protección de las redes informáticas de la Fuerza, con la misión de proteger al Estado Mayor del Ejército y después, extenderse a las grandes Unidades de la Fuerza.

En este sentido se encuentra operando a través de la Oficina Nacional de Tecnologías de Información (ONTI), organismo que depende de la jefatura de gabinete de la secre-

taría de la Función Pública, y donde están establecidas cuáles son las amenazas que existen.

Finalmente en materia de organización la República Argentina crea por la Decisión Administrativa 15/2015 (Ministerio de Defensa, 2015), la Dirección General de Ciberdefensa, la cual llevara a cabo las siguientes acciones:

- Asistir en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar.
- Entender en la coordinación con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica.
- Intervenir en la orientación, dirección y supervisión de las acciones en materia de ciberdefensa ejecutadas por el Nivel Estratégico Militar.
- Ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas.
- Intervenir en la evaluación y aprobación de los planes militares de desarrollo de capacidades de ciberdefensa, en la doctrina básica y en las publicaciones militares pertinentes, cualquiera sea su naturaleza.
- Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.
- Fomentar políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado.

- Promover vínculos sistemáticos de intercambio y cooperación en materia de ciberdefensa con los ámbitos académico, científico y empresarial.
- Impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados.
- Asistir en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa de conformidad a los lineamientos del Ciclo de Planeamiento de la Defensa Nacional.

De lo expresado se considera en forma palpable un trabajo mancomunado entre ambos países, donde la República Argentina aún se encuentra un peldaño por debajo de Brasil, pero en una dirección de trabajo y políticas de estado que en un futuro no tan lejano darán resultados satisfactorios en materia de ciberdefensa.

Conclusiones parciales

Surge una diferencia fundamental del espacio cibernético respecto a los preexistentes. Así como los espacios aéreo, marítimo y terrestre, el entorno es algo que existe en la naturaleza y al que el ser humano tiene que adaptar medios artificiales para su utilización, el ciberespacio es un espacio creado por el hombre y por lo tanto su diseño, son fruto del esfuerzo humano y responden a unas circunstancias que se dieron en el momento de su diseño y desarrollo.

Entender un domino del ciberespacio no solo por parte de la República Argentina, sino que también entre varios países dentro del marco regional, ya que aún no se lo considera a este nuevo escenario con límites tangibles y claramente determinados. Lo que se deberá en este contexto realizar la búsqueda de un trabajo mancomunado por parte de los países de la región a fin de controlar y proteger el espacio cibernético de cualquier amenaza y ciberataque.

En este sentido, se interpreta al ambiente donde se llevan a cabo las operaciones de ciberdefensa, como el espacio cibernético o ciberespacio. Siendo este el domino global dentro de un entorno cibernético, comprendido por infraestructuras críticas, que incluyen redes de telecomunicaciones, sistemas de información y redes informáticas todo ello integrado con sus usuarios y operadores.

Operaciones de ciberdefensa en el campo de combate moderno

En el capítulo anterior se ha intentado demostrar que el ciberespacio es un sistema emergente de la conexión de dos sistemas de diferente naturaleza, el social y el tecnológico, y las posibilidades emergentes del primero están en función de los desarrollos que se dan en el segundo.

Ambos sistemas presentan condiciones de desarrollo dispares en las distintas unidades de análisis a donde se lleve el foco de atención, sean estas políticas, económicas, sociales o militares, entre otras.

En este capítulo se buscará vincular aquellas acciones y actividades que se desarrollan y ejecutan en el denominado ciberespacio, en el cual se manifiestan distintas actividades y acciones, centradas en las medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, e incluye las capacidades de reacción y ataque propias de un conflicto armado.

Los ataques procedentes del ciberespacio pueden adoptar diversas formas: el secuestro clandestino de un sistema, la denegación de servicio, la destrucción o robo de datos sensibles, la piratería de las redes de telecomunicaciones (hacking), la penetración en la protección de los programas informáticos (cracking) y la manipulación fraudulenta de las conexiones telefónicas (phreaking) como por ejemplo, el sabotaje y secuestro de las centrales telefónicas. Todos estos ataques tienen consecuencias negativas para las organizaciones e individuos que los padecen.

En tal sentido, la Directiva de Política de Defensa Nacional de la República Argentina (DPDN), que presenta el Decreto 2645/14 (Ministerio de Defensa, 2015), interpreta que dentro de las operaciones cibernéticas, solo una porción afecta la defensa nacional, y que en ciberdefensa existen dificultades para localizar o determinar si la agresión es militar estatal externa.

En función del marco normativo y doctrinario del Sistema de Defensa Nacional de la República Argentina, se entenderá por ciberdefensa a las acciones y capacidades desarrolladas por el instrumento militar en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo.

La ciberdefensa va mucho más allá de unas meras medidas estáticas preventivas, abarca también medidas que se adaptan al carácter cambiante de las amenazas y del ciberespacio.

Estas acciones son necesarias para la obtención de una capacidad de ciberdefensa militar que cumpla con los objetivos especificados en el concepto de ciberdefensa militar, tales como: garantizar el libre acceso al ciberespacio con el fin de cumplir las misiones asignadas a las fuerzas armadas, obtener analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad, ejercer la respuesta oportuna, legítima y proporcionada ante las amenazas.

Entre sus cometidos, se destacan el garantizar el libre acceso al ciberespacio, la disponibilidad, integridad y confidencialidad de la información, la disponibilidad e integridad de los servicios, la obtención y análisis de la información sobre ciberataques e incidentes así como ejercer una respuesta ante ellos.

Las operaciones cibernéticas

Según Stel (2005), las operaciones cibernéticas se encuentran en estado de evolución, donde algunas se han desarrolladas, ensayadas y comprobadas por su eficacia, y otras están siendo diseñadas. Si bien interpreta que no han sido clasificadas en forma precisa, se puede efectuar un primer intento:

Según la naturaleza.

Operaciones de Red. En general son las que se manifiestan en las debilidades de las redes informáticas y posibilitar aprovecharlas para causar daños a los distintos sistemas

civiles y militares de una Nación. El objetivo básico es afectar la red para entorpecer o destruir la capacidad operativa.

Operaciones de información. Se refiere a conflictos amplios entre naciones, sociedades o civilizaciones. El objetivo es dañar, destruir o modificar la información contenida en redes y sistemas para generar un cambio en lo que una población piensa o conoce.

Según la magnitud.

Operaciones específicas. Son ataques dirigidos contra un blanco puntual, individualizado y específico. Apunta a una persona o pequeños grupos sin alcanzar a una institución.

Operaciones institucionales. Son operaciones que desarrollan las instituciones, organizaciones y entes nacionales o extranjeros de gran magnitud, recurriendo a cualquier tipo de las actividades comprendidas dentro del concepto de devastación cibernética.

Operaciones globales. Son aquellas desarrolladas entre naciones como un todo e incluyen muchos campos del quehacer nacional.

Por otra parte se considera a lo expresado por Carneiro (2012) en su trabajo de investigación, en el cual da otra respuesta a las operaciones de ciberdefensa. En donde se interpreta a las acciones para contrarrestar los ataques cibernéticos y la explotación de los dispositivos, redes informáticas y de comunicaciones de computación, como una actividad permanente. A continuación se muestra la correlación de las acciones de la guerra cibernética:

Exploración cibernética. Consiste en la recopilación de datos negados, evitando el seguimiento; levantar características y vulnerabilidades de los sistemas de destino; obtener las características ("Firma Digital") de sistema de destino.

Ataque cibernético. Será el empleo de herramientas informáticas para cambiar y destruir datos, reducir la eficacia de los sistemas informáticos y dañar sistemas informáticos y estructuras físicas.

Protección cibernética. Serán aquellas acciones o esfuerzos a proteger de las redes contra los ataques cibernético realizado por oponente.

En lo que respecta a la Argentina, el interrogante que surge frente a este trabajo, es si el país está en capacidad de realizar algún tipo de operación cibernética. Consultado el Coronel García, antes citado, confirmó que desde el punto de vista de la ciberdefensa militar, hoy no existen acciones en capacidad de realizarse debido a que no existe doctrina aprobada de ciberdefensa. Si está en ejecución, a partir de la creación del Comando Conjunto de Ciberdefensa, la implementación de un Plan de Desarrollo de la Capacidad, el cual abarca el corto, mediano y largo plazo, y está, en este momento, sujeto a la aprobación del Ministerio de Defensa de la Nación. Puede destacarse que ya existe, en el ámbito del Estado Mayor Conjunto de las Fuerzas Armadas (EMCFFAA) y cada una de las fuerzas, tienen órdenes particulares vinculadas a las medidas de seguridad informática, las cuales pueden considerarse componentes del todo que es la ciberdefensa. (Comando Conjunto de Ciberdefensa, comunicación personal, febrero 2015).

La ciberdefensa

Conceptos generales. La descripción y conceptualización del ciberespacio realizada en el capítulo anterior, dan el marco referencial en donde tendrán lugar las acciones y actividades cibernéticas, las que deberán ser claramente planeadas, conducidas, controladas y supervisadas por el comandante.

En este ambiente, es imposible distinguir con claridad al agresor, sus fines son casi siempre desconocidos; por la facilidad de acceso y bajo costo, cualquier individuo u

organización con conocimientos mínimos, puede efectuar ataques en este ambiente que podrían tener efectos devastadores en cualquier estado.

Por otra parte, el empleo de sistemas y redes informáticas por parte de las fuerzas terrestres, las hace objeto de amenaza en este nuevo ambiente, por lo que será imprescindible su organización, equipamiento y adiestramiento para operar en el ciberespacio, ya sea en tiempos de paz, para la protección de sus propios sistemas y eventualmente para la neutralización y/o afectación de los sistemas informáticos enemigos, en la ejecución de operaciones militares.

Expresa el Reglamento de Conducción para las Fuerzas Terrestres (2015), en caso de conflicto la defensa cibernética, será una operación que complementará al resto de las operaciones tácticas y eventualmente a las subsidiarias en tiempos de paz.

Aunque la defensa cibernética se estructura, planifica y coordina desde el máximo nivel de conducción, su ejecución se concreta en todos los ámbitos del estado y en todos los niveles.

Por consiguiente, cada elemento de las fuerzas terrestres, equipado con sistemas informáticos, o integrado a redes informatizadas, tendrá responsabilidad directa en el cumplimiento de dichas normas y procedimientos para asegurar el normal funcionamiento de los sistemas, redes y mantener el control del espacio cibernético de interés para las fuerzas terrestres.

Desde esta perspectiva, la ciberdefensa comprende medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, como así también la capacidad de reacción y ataque propios de un conflicto armado. Desde un fundamento concreto, la ciberdefensa se sustenta mayoritariamente en tecnología de ciberseguridad ampliamente probada y desplegada en el sector civil. (Lopez Hernández Ardieta, 2013).

Todo ello conforma un escenario de nuevos riesgos para el que es necesario que los distintos gobiernos desarrollen planes o estrategias, y se contemple a las ciberamenazas como un riesgo al que es preciso hacer frente para la mejora de la seguridad nacional.

Finalidad y modalidades de la defensa cibernética. La defensa cibernética es el conjunto de acciones desarrolladas en el ciberespacio para prevenir y contrarrestar toda amenaza o agresión cibernética. Así lo conceptualiza el Reglamento de Conducción para las Fuerzas Terrestres (2015).

Tiene dos modalidades, defensa directa e indirecta. La finalidad de la primera es vigilar y controlar las redes y sistemas en los ámbitos específico y conjunto.

La defensa cibernética indirecta, tiene por finalidad disputar el control del ciberespacio necesario para el accionar de las fuerzas militares.

Para cumplir estas funciones, los elementos de ciberdefensa que se organicen deberá satisfacer las exigencias del comandante y su estado mayor solo así podrán cumplir con la finalidad expresada, operando, controlando y accionando por medio de centros de ciberdefensa, evitando acciones contra el comando y control, que puedan desarticular la conducción del comandante, buscando en todo momento la seguridad del ciberespacio, mediante acciones cibernéticas que brinden libertad de acción a las operaciones.

Las medidas de seguridad y los procedimientos de comando y control serán medidas de naturaleza defensiva, adoptadas para reducir la vulnerabilidad del sistema propio a la explotación que pueda realizar el enemigo.

Planeamiento y Ejecución. Para comprender estos aspectos, se considera lo expresado en el Reglamento de Conducción para las Fuerzas Terrestres (2015), teniendo en cuenta que las operaciones de defensa cibernética desde el nivel operacional hacia los menores niveles, la totalidad de los comandantes o jefes y sus órganos de asesoramiento y asistencia, deberán considerar en forma permanente, los riesgos existentes para el de-

sarrollo de otras operaciones en caso de que sus fuerzas, sean blanco de ataques cibernéticos. Asimismo, deberán adiestrar a sus fuerzas para que además de saber combatir con los sistemas informáticos existentes, puedan operar con procedimientos manuales alternativos en caso de que los sistemas informáticos en uso, hayan sido afectados.

La elaboración de normas y procedimientos de seguridad informática, deberán incluir aquello relacionado al empleo de sistemas con posibilidad de transmisión de datos, incluyendo sistemas de control de tiro, sistemas de vigilancia electrónica, de comunicaciones, de comando y control y medios de comunicación personales. Esto permitirá en las operaciones un control del sistema cibernético, como así también mantener un ciberespacio seguro.

El apoyo de Comunicaciones e Informática en operaciones de defensa cibernética. Siguiendo el Reglamento de Conducción para las Fuerzas Terrestres (2015), mantiene que el apoyo de comunicaciones e informática se materializará mediante la instalación, operación y mantenimiento de redes informáticas que se integrarán y serán parte del ciberespacio, ámbito donde se desarrollarán las operaciones de ciberdefensa. Siendo de esta manera prioritaria para el comando y control del comandante en el campo de combate moderno.

Además de la instalación y mantenimiento de las redes, a través de las cuales se ejecutará la defensa cibernética, resultarán esenciales las actividades y tareas de seguridad informática o seguridad en redes, que son el principal componente de las denominadas operaciones de ciberdefensa directa.

La seguridad informática se proporcionará a través de distintos procedimientos, tales como la protección física, que abarca a las bases de datos, los servidores de los centros de datos principales y de alternativa en guarnición y aquellos establecidos en campaña y la protección a los enlaces tanto físicos como no cableados de las redes informáticas.

La protección lógica, que se brinda por medio de software para seguridad en los accesos a la red (proxis, firewall) y software antivirus, malware, etc.

La protección de empleo o utilización, que se logra mediante el cumplimiento de las directivas, normas y procedimientos operativos normalizados en vigencia y el adecuado manejo de los niveles de información.

La seguridad informática, que requiere una permanente actualización en el desarrollo de herramientas y aplicaciones con ese fin sumado a la conciencia de los usuarios para proteger la información y los sistemas frente a los ataques que sufran las redes.

El cumplimiento de estos procedimientos desde el centro neurálgico de un sistema hasta el menor nivel de ejecución (usuario), contribuirán al comandante en todo momento la libertad de acción y la seguridad que le permita la conducción de las fuerzas terrestres en busca del logro del objetivo.

La ciberdefensa en apoyo a las operaciones tácticas

Las acciones cibernéticas se manifiestan y se ejecutan en las distintas operaciones tácticas, como operaciones de configuración y protección. Como en las operaciones ofensivas, donde se las emplea como seguridad, con el propósito de evitar la interferencia imprevista del enemigo, mantener la integridad del dispositivo y asegurar el mantenimiento de la libertad de acción. De esta manera se considera en el Reglamento de Conducción para las Fuerzas Terrestres (2015).

Es de particular importancia la adopción de medidas para la protección de todos los sistemas informáticos y otros que recurran a emisiones electromagnéticas, electroópticas y acústicas, de las acciones de guerra cibernética y/o guerra electrónica que ejecute el enemigo, aunque esta consideración es de aplicación a la totalidad de las actividades que realicen las fuerzas terrestres.

Las operaciones de ciberdefensa, serán aplicadas en las operaciones de interdicción, como una acción cibernética. Será ejecutada en forma complementaria a cualquiera de las operaciones. En el caso de la cibernética, por medios del nivel estratégico, aunque sus efectos incidan en el nivel operacional y táctico. Normalmente serán conducidas por el nivel estratégico aunque su ejecución se realice en forma descentralizada.

Siguiendo al Reglamento de Conducción para las Fuerzas Terrestres (2015), menciona que durante el planeamiento se deberá tener en cuenta que el enemigo conocerá las vulnerabilidades de las vías de comunicación que se emplearán, adoptará seguramente medidas para evitar o reducir cualquier acción de interdicción propia. En tal sentido, el valor de la interdicción electrónica/cibernética, aumentará en tanto contribuya mediante la afectación de su comando y control, al limitar la capacidad de reacción del enemigo. Por otra parte, la ejecución de operaciones de velo y engaño como complemento de esta operación, aumentará la probabilidad de que su ejecución sea exitosa.

Se deberá tener en cuenta que en toda operación táctica será necesario un apoyo de defensa cibernética que contribuyan a garantizar la libertad de acción en las operaciones militares y proporcionen un adecuado nivel de seguridad en el empleo de los sistemas propios.

Para ello una fuerza deberá contar con ciertas capacidades cibernéticas que cumplan en una primera clasificación, como las que se mencionan a continuación:

La defensa, que incluya las medidas para la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, que puedan comprometer la información y los sistemas que la manejan. La explotación, que permita la recopilación de información sobre sistemas de información de potenciales enemigos y por último la respuesta, que incluya las medidas y acciones a tomar ante amenazas o ataques. (Pastor Acosta, 2012).

A fin de abonar lo expresado, se debe tener en cuenta la utilización de acciones de ciberdefensa como parte de una operación principal ya sea con una actitud ofensiva como defensiva, contribuyendo a esta a fin de buscar dislocar el comando y control del adversario.

La conducción de la ciberdefensa

En busca de una conducción eficiente en las operaciones de ciberdefensa, el comandante deberá aplicar ciertos principios. Ellos estarán dados por la vinculación de los principios para conducir las operaciones militares, conjuntamente con los preceptos para conducir las operaciones militares y en un segundo plano los conceptos rectores del apoyo de teleinformática.

Para una interpretación de estos, se los relacionará con la ciberdefensa, buscando una vinculación en esta materia a fin de contribuir a la conducción del comandante en el campo de combate moderno.

Principios para conducir las operaciones militares. Se considera para este tema el Reglamento de Conducción para las Fuerzas Terrestres (2015), donde manifiesta que un principio militar es un axioma o verdad fundamental, cuya observancia posibilita, en gran medida, el ejercicio de una exitosa conducción de las fuerzas en el cumplimiento de una misión.

Los principios no constituyen un dogma, ni tienen la intención de establecer restricciones a la libertad de acción de un comandante. Balancear las exigencias y requerimientos de su aplicación constituye la esencia del éxito operacional. Por lo tanto, no deben ser usados como una lista de chequeo ni se aplican de la misma manera a cualquier situación.

Si bien es cierto que su aplicación no debe ser dogmática y que además no asegurarán por si solos el éxito al comandante, sí se puede certificar que la omisión del o los

que correspondan a un caso particular dificultarán el accionar o lo conducirán normalmente al fracaso.

El Ejército Argentino reconoce como principios de aplicación en la conducción de las operaciones en el ámbito terrestre los siguientes:

Voluntad de vencer, Economía de Fuerzas, Maniobra, Objetivo, Sorpresa, Masa/Concentración, Unidad de comando, Seguridad, Libertad de acción, Ofensiva, Simplicidad, Sostenimiento e Integración.

Algunos de estos principios que se han expresado, se los puede vincular con ciertas acciones de ciberdefensa a fin de lograr una mejor interpretación de los mismos. (Ver Cuadro 1).

Cuadro 1: Vinculación de los principios con la ciberdefensa

Ofensiva	Ataque distribuido de negación de servicio en Estonia en 2007 sobrecargando las redes del país.
Masa	Presuntos ataques preventivo por actores rusos en redes de Georgia, a fin de detener fuerzas georgianas durante la invasión del 2008
Unidad de Comando	La utilización de un control de red de información global a través de un Equipo de Trabajo designado.
Seguridad	Proteger y permitir la operatividad de las redes de comando y control por medio de defensas en capas y configuraciones seguras.
Sorpresa	Ataques cibernéticos no anunciado a sistemas vulnerables o comprometidos.
Libertad de Acción	Ejecutar operaciones cibernéticas que permitan lograr aplicar el poder de combate disponible según la propia intención.

Fuente: Elaboración personal.

Preceptos para conducir las operaciones militares. En función a lo normado por el Conducción para las Fuerzas Terrestres (2015), se considera a estos preceptos como una orden o mandato relativo a una conducta e impuesto o establecido por una autoridad. Son las instrucciones o reglas que se establecen para la conducción de operaciones militares.

Estos preceptos se construyen sobre los principios de la conducción. Describen la ejecución exitosa de las operaciones y su observación es esencial para la consecución de la victoria. Si bien no garantizan el éxito, su ausencia incrementa el riesgo de derrota.

Al igual que sucede con los principios, la elección y aplicación de uno o más preceptos dependerá del tipo de operación militar para desarrollar y, especialmente, de la existencia o no de una voluntad oponente.

El Ejército Argentino reconoce como preceptos para conducir las operaciones militares en el ámbito terrestre los siguientes: Iniciativa, Velocidad, Profundidad, Sincronización y Flexibilidad. (Ver Cuadro 2).

Cuadro 2: Vinculación de la ciberdefensa con los preceptos de la batalla

Velocidad	Actuar más rápido que el enemigo, como por ejemplo utilizando ataques DDoS hasta que sean deliberados y específicamente contenidos.
Flexibilidad	Operaciones cibernéticas flexibles y versátiles actúan como un multiplicador del poder de combate de las fuerza, a fin de contar con una capacidad de adaptación a diferentes cambios de situación.
Profundidad	Acceder al hardware y software del adversario con el fin de garantizar el acceso necesario hasta el Comando y Control de este, logrando la extensión de las operaciones en tiempo, en espacio y en medios.
Iniciativa	Atacar las redes del adversario con el fin de detectar, impedir, negar, y derrotar a las acciones del enemigo y su libertad de acción, a fin de permite anticiparse inteligentemente a los hechos y suponer la puesta en práctica del espíritu ofensivo.
Sincronización	Ejecutar una seria de acciones cibernéticas en el ciberespacio enemigo, las cuales presenten distintos efectos en forma simultáneos, para concentrar en oportunidad y en el lugar decisivo el mayor poder de combate relativo.

Fuente: Elaboración personal.

Conceptos rectores del apoyo de teleinformática. Siguiendo al Reglamento de Conducción de Comunicaciones (2001), establece que son pautas probadas que deberán ser interrelacionadas, balanceadas y aplicadas en la planificación y ejecución del apoyo a las operaciones, para lograr que el mismo se desarrolle en forma eficaz. Su observancia, con relación a los principios para conducir las operaciones, facilitará el accionar del

comandante y contribuirá al éxito en el cumplimiento de la misión. En este sentido se considera como conceptos rectores a los que se detallan a continuación: Confiabilidad, Seguridad, Rapidez, Economía, Flexibilidad, Integración, Dispersión, Elección de la facilidad apropiada y Facilidades orgánicas. (Ver Cuadro 3).

Si bien estos conceptos guardan una relación directa con el apoyo y diseño de teleinformática, se puede considerar que algunos de ellos deben ser considerados por su vinculación con la acciones de ciberdefensa en el campo de combate moderno.

Cuadro 3: Conceptos rectores y su vinculación con la ciberdefensa

Seguridad	Aplicar medidas y técnicas de protección, tanto para negar al enemigo toda información, como para impedir el acceso a redes informáticas. Proporcionará libertad de acción y seguridad en las operaciones y contribuirá al logro de la sorpresa.
Flexibilidad	Adecuar la distribución de centros de respuesta que permitan que un sistema cibernético, sin modificaciones sustanciales, pueda adaptarse rápidamente a las variaciones operacionales que, razonablemente, puedan presentarse en combate.
Rapidez	Lograr la capacidad del manejo y transmisión de la información, en el tiempo oportuno. Mediante un ciberespacio confiable y seguro.
Integración	Habilitar el acceso recurrente a redes específicas, sistemas o nodos tanto por medios remotos o de manera directa con el fin de garantizar el acceso necesario para que las acciones cibernéticas logren una integración rápida y flexible en los sistemas del campo de combate.

Fuente: Elaboración personal.

Consultado el Coronel García sobre las acciones de ciberdefensa que podrá ejecutar el comandante, expresó que la ciberdefensa es un sistema de armas, transversal a los componentes y sus posibles combinaciones. No puede hablarse de dominio en el mismo sentido que, por ejemplo, se habla del dominio del espacio aéreo.

El espacio cibernético es muy próximo a lo infinito, por lo tanto, un Comandante debe ocuparse de brindar la máxima protección posible de sus sistemas, especialmente los que posibilitan el comando y control. Una vez determinada la doctrina pertinente, ejecutar las operaciones necesarias que afecten el comando y control del comandante enemi-

go. Nótese que esto no implica necesariamente destruir sus sistemas, sino obtener información o limitar el acceso del enemigo a su información almacenada o en tránsito. (Comando Conjunto de Ciberdefensa, comunicación personal, febrero de 2015).

Conclusiones parciales

Las acciones de ciberdefensa deberán estar bajo un precepto o mandato, instrucciones o reglas que se establezcan para la conducción de operaciones cibernéticas, construidos sobre los principios de la conducción que si bien no garantizan el éxito, su ausencia incrementa el riesgo de derrota.

De lo expresado se interpreta que dentro del ciberespacio se accionará por parte del comandante mediante operaciones de ciberdefensa, en donde deberá aplicar ciertos principios y preceptos para ejercer la conducción de las mismas en forma eficiente.

Para la conducción de sus fuerzas, el comandante aplicará el uso de estas operaciones de ciberdefensa, buscando en todo momento un ciberespacio seguro y confiable a fin de lograr la libertad de acción.

Conclusiones

A lo largo del presente trabajo se han analizado dos aspectos fundamentales en materia de ciberdefensa, en relación con la conducción del comandante. En primer término, se analizó el ciberespacio y luego aquellas acciones que se ejecutan en él. Se definió el ciberespacio como el espacio donde se desarrollan acciones cibernéticas, en el cual el comandante deberá ejecutar operaciones de ciberdefensa a fin de lograr un espacio seguro y confiable.

Por otro lado, se conceptualizó al ciberespacio como el ámbito virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de información y comunicaciones, aunque sus implicancias se darán en el ambiente físico.

Lo analizado permitió identificar las acciones que son llevadas a cabo en el ciberespacio, entendiendo que la ciberdefensa va mucho más allá de unas meras medidas estáticas preventivas y debe englobar también medidas que se adapten al carácter cambiante de las amenazas y del espacio cibernético.

Estas acciones son necesarias para lograr una capacidad de ciberdefensa militar que cumpla con los objetivos especificados en el concepto, como son: garantizar el libre acceso al ciberespacio con el fin de cumplir las misiones asignadas a las Fuerzas Armadas, obtener analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad, ejercer la respuesta oportuna, legítima y proporcionada ante amenazas.

No obstante las operaciones cibernéticas en el campo de combate moderno se encuentran en constante evolución, las que inciden directamente en el comando y control.

En donde al agresor es casi imposible distinguirlo con claridad, sus fines son casi siempre desconocidos. Teniendo en cuenta que la facilidad de acceso y bajo costo permite a cualquier individuo u organización con conocimientos mínimos, puede efectuar ataques en el ciberespacio los que podrían tener efectos devastadores en cualquier conflicto.

Por lo expuesto es de consideración que las acciones que debe adoptar el comandante en este espacio (ciberespacio), en un tiempo determinado y con sus medios a disposición. Para lo cual accionará por medio de operaciones cibernéticas a fin de prevenir y contrarrestar toda amenaza o agresión cibernética.

En el marco de las mencionadas operaciones de defensa cibernética, se debe contar con la aplicación de ciertos principios básicos, entendiendo por estos a la vinculación entre los principios para conducir las operaciones militares, los preceptos de las operaciones y los conceptos rectores del apoyo de teleinformática.

Por ello, que el comandante deberá aplicar en la conducción y ejecución de las operaciones los principios básicos a fin de desorganizar y destruir el centro de gravedad del enemigo, como así también, dar protección y seguridad al ciberespacio que le permita contar con una amplia libertad de acción en el campo de combate moderno, siendo estos los siguientes principios:

Seguridad: Resulta de la adopción de un conjunto de medidas destinadas a prevenir la sorpresa, preservar la libertad de acción y negar al enemigo información sobre las propias fuerzas, manteniendo un ciberespacio confiable y seguro a fin de limitar acciones cibernéticas por parte del enemigo. Con la finalidad de proteger y preservar todos aquellos medios, infraestructuras críticas e información, contenida en el ciberespacio.

Así mismo se busca proteger y permitir un sistema operable de redes de comando y control, a través de defensas en capas y reconfiguraciones robustas y auto ajustable

Este principio estará directamente en relación con la libertad de acción, el que se verá favorecido por el mantenimiento de la iniciativa y evitará ser sorprendido por ataques cibernéticos. En tal sentido, este principio permite lograr los propios objetivos, a pesar de las interferencias del oponente. Negar propia información, contribuye a una adecuada seguridad la que permite tomar decisiones rápidas y acertadas.

Libertad de acción: será la facultad de aplicar el poder de combate cibernético disponible según la propia intención, sin que el enemigo, por sus medios o por efecto de su conducción, pueda impedir que así suceda. Originadas en factores de la situación tales como: la conducción del oponente, el ciberespacio o las configuraciones de las capacidades de los medios propios.

Será el principio permanentemente buscado en este tipo de operaciones, como resultante del resto de los principios básicos que aplicará el comandante. Siendo su propósito el de disponer de una situación militar favorable que permita la aplicación del poder de combate libre de obstáculos, ciberamenazas o ciberataques.

El mantenimiento de la iniciativa, la observancia del principio de seguridad y el ejercicio de la sorpresa, será la resultante de una adecuada libertad de acción.

Finalmente, es indudable que el principio de la conducción más importante es el de libertad de acción, ya que cualquier operación que se trate y se ejecute en el ciberespacio, afectará en forma más o menos decisiva la libertad de acción del comandante beneficiado o afectado con ellas.

Por lo expuesto anteriormente se considera necesario destacar la necesidad de contar con estos principios para la conducción del comandante, los que le proporcionarán a este un ciberespacio seguro y confiable, como así también la libertad de acción en las operaciones, manteniendo la iniciativa en búsqueda de la ofensiva en logro de alcanzar la victoria.

Referencias

Bejarano M. J. (2011). *Protecciones de las infraestructuras críticas*. España: Instituto de Ingeniería Eléctrica y Electrónica (IEEE)

Carneiro, J. M. (2012). *A Guerra Cibernética: uma proposta de elementos.* Río de Janeiro: ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO.

Clarke, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. Estados Unidos: ECCObooks.

Cloud, J. (2007). *Integrated Cyber Defenses: Towards cyber defense doctrine.* Naval Postgraduate School, California, EEUU.

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

Ejército Argentino. (2001). *Conducción de comunicaciones (ROD-05-01).* Buenos Aires, Argentina: Departamento Doctrina.

Hernández-Ardieta, D. (2013). *Capacidades esenciales para una ciberdefensa nacional.* Panamá: Indra

Honorable Congreso de la Nación (1988). Ley de Defensa Nacional Nº 23.554. *Boletín Oficial Nº 26375*, p4. Buenos Aires, Argentina.

Kuehl, D. (2009). *From Cyberspace to Cyberpower: Defining the problem, information resources management.* College-National Defense University, EEUU.

Lorents, O. R. (2010). *Cyberspace: Definitions and Implications. Cooperative Cyber Defence Center of Excellence.* Estonia: Tallinn.

Ministerio de Defensa. (2014). *Informe de Investigación. Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo*. Escuela de Defensa Nacional. Buenos Aires, Argentina.

Ministerio de Defensa. (2015). *Directiva de Política de Defensa Nacional.* Buenos Aires, Argentina: Min Def.

Ministerio de Defensa. (2014). *Doctrina Básica para la Acción Militar Conjunto (PC 00-01).*Buenos Aires, Argentina, EMCO.

Ministerio de Defensa (2010). *Libro Blanco de la Defensa.* Buenos Aires, Argentina.

Ministerio de Defensa (2014). Creación del Comando Conjunto de Ciberdefensa. *Resolución MINDEF 343/ 14May14*. Buenos Aires, Argentina.

Ministerio de Defensa (2015). *Creación de la Dirección General de Ciberdefensa. Decisión Administrativa n° 15/2015.* Buenos Aires, Argentina.

Ministerio de Defensa. (2008). *Estrategia de la Defensa Nacional.* Brasil: Mind Def.

Ortiz, J. U. (2012). Estrategia de Defensa Cibernética en la Era de la Información. *La Revista ESG*, p89. Buenos Aires, Argentina.

Palacio, J. E. (2012). *Evolución del Ejército Argentino en seguridad informática en el marco de operaciones militares llevadas a cabo en el ciberespacio*. Instituto Universitario del Ejército, Escuela Superior de Guerra, Buenos Aires, Argentina.

Poder Ejecutivo Nacional (2015). Directiva de Política de Defensa Nacional. *Boletín Oficial Nº 33052*. Buenos Aires, Argentina.

Pastor Acosta, O. (2015). *Capacidades para la defensa en el ciberespacio.* Centro Superior de Estudios de la Defensa Nacional. Ministerio de Defensa, España.

Real Academia Española. (2012). *Diccionario de la lengua española* (22.aed.). Recuperado en http://www.rae.es/rae.html

Stel, E. (2005). *Guerra Cibernética.* Buenos Aires, Argentina: Círculo Militar.

Touré, H. (2011). *La Búsqueda de la Paz en el Ciberespacio.* Suiza: Unión Internacional de Telecomunicaciones (UIT).

Zakon, R. H. (1997). RFC 2235 - *Hobbes' Internet Timeline*. EEUU: Network Working Group.