ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA:

La ciberdefensa

TÍTULO:

La ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del teatro de operaciones

AUTOR: Mayor Luis Javier Anca

Año 2015

Aclaración

Las opiniones, análisis e interpretaciones expresadas en el presente trabajo académico son exclusivos del autor, y no reflejan necesariamente políticas oficiales ni posición, tanto de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas como del Ejército Argentino.

RESUMEN

Hoy en día, se está asistiendo a la necesidad de controlar los riesgos informáticos operacionales debido a la utilización extensiva de las nuevas tecnologías, a la existencia de una infraestructura de información mundial y a la aparición de nuevos riesgos.

Tal es así que la amenaza de un conflicto cibernético nunca ha tenido tanta trascendencia debido a los adelantos tecnológicos y a la creciente infraestructura digital que han hecho a las Fuerzas Armadas, depender de sistemas entrelazados y complejos.

El presente trabajo analiza la ciberdefensa vinculada con la conducción dentro del teatro de operaciones, a fin de determinar los principios de la guerra a aplicar por el comandante para lograr una interoperabilidad conjunta.

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 nivel operacional.

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

Este nuevo desafío para el teatro de operaciones exige de la interacción en virtud de una operación eficiente, en donde surge el concepto de interoperabilidad en función a los principios de la guerra como herramienta para el logro de una ciberdefensa conjunta y capaz de lograr neutralizar las amenazas en cada nivel del ciberespacio.

Por lo expuesto, se plantea como objetivo del presente trabajo, determinar aquellos factores esenciales que permitan la interoperabilidad en materia de ciberdefensa dentro de un teatro de operaciones y como así también analizar los diversos principios de la guerra que hacen una ciberdefensa interoperable.

Palabras clave: Ciberdefensa – Interoperabilidad – Ciberespacio – Teatro de Operaciones.

Tabla de Contenido

INTRODUCCIÓN

Históricamente, las guerras han configurado, junto con el comercio o la diplomacia, una de las principales formas de relación entre los Estados. Para Clausewitz, "la guerra no es solamente un acto político, sino un verdadero instrumento político, una continuación de las relaciones políticas, una gestión de las mismas por otros medios".[1]

Consecuentemente, las formas de hacer la guerra en un pasado no tan remoto, ha sido enmarcada en tres dimensiones, en donde las acciones principales estaban materializadas por las grandes maniobras operacionales en función de los medios a disposición.

Lo expresado anteriormente se denomina guerra convencional, mediante el uso de medios y tácticas tradicionales, entre dos o más Estados abiertamente hostiles y bien definidos. Este tipo de guerra excluye el uso de armas de destrucción masiva y específicamente el uso de armas nucleares.

En general, el propósito de la guerra convencional es debilitar o destruir las fuerzas militares del enemigo, para negarle la posibilidad de seguir combatiendo y obligar a sus gobernantes a rendirse.

El paso de los años y la evolución de la tecnología fueron transformando la forma de hacer la guerra luego de la Segunda Guerra mundial. En ese sentido, se ha ido transformando el campo de combate con el surgimiento de un nuevo domino al que se conoce como ciberespacio.

El presente trabajo cuenta con la temática central en materia de ciberdefensa en relación a la interoperabilidad conjunta en el teatro de operaciones (TO). Para el desarrollo de este trabajo, se entiende la existencia de uno de los principales problemas que es la ausencia de bibliografía respecto del tema seleccionado.

En lo que respecta a la investigación del trabajo, se considerará la bibliografía de Jeffrey Carr[2] titulada "Inside Cyber Warfare", como así también todo aquello relacionado con ciberdefensa publicado por Hamadoun Touré[3] en la Unión Internacional de Telecomunicaciones.

---

[1] Clausewitz, Karl; *De la Guerra*, Buenos Aires, Editorial Need, 1998, Libro Primero, Cap. I, Pág. 41.
[2] Carr, Jeffrey; analista de la ciberseguridad, fundador y principal investigador del proyecto Grey Goose donde se ha llevado a cabo una investigación en conflictos cibernéticos incluyendo los ataques rusos cibernéticos en Georgia.
[3] Touré, Hamadoun; secretario general de la Unión Internacional de Telecomunicaciones (UIT) y del

En el ámbito de la Escuela Superior de Guerra del Ejército (ESGE), se han realizado trabajos y artículos[4] [5] abordando aspectos referidos al ciberespacio, a la interoperabilidad de los sistemas, y otros referidos a la revolución de asuntos militares y nuevas tecnologías.

Del mismo modo, pero en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas (ESGCFFAA), se realizaron trabajos finales de donde se extraen las siguientes conclusiones respectivamente:

> *El empleo efectivo de los medios y tecnologías cibernéticas facilitan y favorecen el dominio de las FFAA en un TO, siempre y cuando se sustenten en estructuras orgánicas con la adecuada distribución personal. Además contar con esta capacidad disuade al potencial enemigo de escalar una crisis por temor a la desarticulación de su centro de comando y control.*
>
> *Contar con la capacidad de combatir y defenderse contra un ataque cibernético debería ser un objetivo primordial para el estado nacional y una misión de las FFAA, para ratificar la seguridad, supervivencia, estabilidad y defensa del estado.*
>
> *Es necesario para el desarrollo de medidas de seguridad, formar profesionales especializados, supervisar la aplicación de medidas de seguridad cibernética, adquisición de tecnología y contratación de servicios especializados con el respectivo análisis de riesgos ante un ataque cibernético.* [6]

En relación al segundo trabajo, se expresan las siguientes conclusiones:

> *Que los conceptos formados a partir y en función de los ámbitos naturales (terrestre, naval, aeroespacial) en los que está inmersa la cotidianeidad, dificultan la visualización y la comprensión del espacio cibernético como un nuevo ámbito de realidad.*

Panel Permanente para la Supervisión de la Seguridad de la Información Federación Mundial de Científicos, referentes de la UIT, en la que la Argentina es firmante y emite documentos y recomendaciones.

[4] Stel, E. *Guerra Cibernética.* Buenos Aires, Argentina; Círculo Militar, Buenos Aires, 2005.

[5] Palacio, J.; *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, 2013.

[6] Giudici, Daniel; La guerra cibernética: lineamientos para la seguridad cibernética en un teatro de operaciones, Trabajo Final Integrador de la Especialización Estratégica Operacional y Planeamiento Militar conjunto; Escuela Superior de Guerra Conjunta; Buenos Aires; 2013.

Los desafíos operacionales en el espacio cibernético dentro del ámbito de la República Argentina, ya han comenzado a establecerse, y al mismo tiempo, los actores involucrados perciben como un beneficio la realización de operaciones ciberespaciales. Cabe aclarar, que gran parte de estos actores poseen un concepto, respecto a las operaciones ciberespaciales, más ligado a la seguridad informática que a la defensa de intereses vitales. [7]

Los cambios constantes en hacer la guerra llevan a la necesidad de actuar en el campo de combate moderno por parte del comandante, ejerciendo la conducción de su fuerza lo más rápida y eficiente posible, teniendo en cuenta un espacio particular denominado ciberespacio.

Hoy no se entiende a los conflictos modernos solo con los espacios tradicionales como tierra, mar y aire, sino que el nuevo ambiente operacional puesto en función con el surgimiento en general de una nueva "Era de las Tecnologías de la Información" que comienza a dejar atrás los alrededor de 200 años de "Era Industrial" y en particular el desarrollo de una nueva etapa de la "Revolución de Asuntos Militares" en el campo de la defensa nacional y la seguridad internacional caracterizadas por un avance tecnológico de gran velocidad, lo que redunda en un nuevo ambiente operacional.

La denominada guerra en este campo como guerra cibernética es eminentemente asimétrica, siendo esta un conflicto violento donde existe una gran desproporción entre las fuerzas tanto militares como políticas de los bandos implicados, y que por lo tanto obliga a explorar dimensiones históricamente aún no conocidas o empleadas. Entre estos medios se cuenta con la guerra de guerrillas, la resistencia, toda clase de terrorismo, la contrainsurgencia y la ciberguerra.

Los hechos sucedidos a nivel mundial fundamentan y justifican el desarrollo de la ciberdefensa en atención a ellos. De estos, se pueden mencionar incidentes de ciberataques y las acciones realizadas por parte sus gobiernos.[8]

En lo que respecta al aporte teórico al campo disciplinario implica un análisis del ciberespacio en función a las actividades de ciberdefensa, mediante una

[7] Cisneros, Ezequiel Rodríguez; Las operaciones ciberespaciales: desafíos operacionales en el espacio cibernético como nuevo campo de lucha; Trabajo Final Integrador de la Especialización Estratégica Operacional y Planeamiento Militar conjunto; Escuela Superior de Guerra Conjunta; Buenos Aires; 2012.

[8] Ver Anexo 1: Principales acciones cibernéticas de importancia en el mundo.

interoperabilidad conjunta que materialice las acciones cibernéticas en el teatro de operaciones.

Con la elaboración de este trabajo de investigación, se pretende extraer las implicancias que surjan de la interoperabilidad en un teatro de operaciones en relación a la ciberdefensa que permita la apertura de nuevas líneas de investigación para profundizar en este tema.

Para ello se considera en una primera aproximación teórica el (ROB 00-01) Conducción para las Fuerzas Terrestres, como así también el (MC 20-01) Estrategia y Planeamiento Nivel Operacional y la (PC 20-01) Planeamiento para la Acción Militar Conjunta Nivel Operacional, donde se puede observar que los mismos hacen referencia a la existencia de los conceptos principales del tema.

En tal sentido, los aspectos centrales que va a tratar el trabajo será la vinculación de los conceptos del ciberespacio, la ciberdefensa, el nivel operacional y su interoperabilidad en el Teatro de Operaciones.

Por otra parte, a fin de dar un límite de investigación al trabajo, se considera que la composición 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 directa 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 alcance comprende el análisis de los principios de la guerra en relación a la interoperabilidad en el teatro de operaciones en materia de ciberdefensa.

El estudio estará circunscrito al campo disciplinar militar, específicamente al nivel operacional y sin involucrar aspectos técnicos tecnológicos. En otro sentido, dado que los elementos del diseño operacional se pusieron en vigencia desde 1990, la investigación histórica será a partir de dicho año.

En aquel espacio cibernético, definido como un nuevo ámbito para efectuar operaciones militares y acciones cibernéticas, plantea un sinnúmero de interrogantes. Entonces, ¿Cuáles son las implicancias operativas de la necesidad de una interoperabilidad conjunta en el teatro de operaciones en relación a las operaciones de ciberdefensa?

Para dar respuesta a este interrogante y dado el carácter de la ciberguerra el objetivo general planteado es el de determinar aquellos factores esenciales que

permitan la interoperabilidad en materia de ciberdefensa dentro de un teatro de operaciones. Para el logro de dicho objetivo, los objetivos específicos se concretan en:

Vincular la ciberdefensa en el marco de un teatro de operaciones y analizar los diversos principios de la guerra que hacen una ciberdefensa interoperable.

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

En lo que respecta a la hipótesis, establece que el empleo del ciberespacio mediante una interoperabilidad conjunta en un teatro de operaciones, derivó en la conformación de una fuerza operacional a fin de actuar en el espacio cibernético mediante acciones de ciberdefensa, hacia el logro de un objetivo común.

En el presente trabajo se recorre, en el primer capítulo, algunas consideraciones sobre la naturaleza del espacio cibernético, la definición del término, el ciberespacio en el teatro de operaciones y los elementos del diseño operacional en relación a la ciberdefensa. En el segundo capítulo, se centrará la atención en los principios de la guerra y la búsqueda de la interoperabilidad en el teatro de operaciones.

CAPÍTULO I

El dominio del ciberespacio en el nivel operacional

1.1 La naturaleza del ciberespacio

El ciberespacio es incorporado en la actualidad como uno más de los llamados Global Commons, tales como tierra, mar y aire.[9]

Sin embargo, hay un factor que distingue al ciberespacio de los otros tres dominios, su carácter artificial le confiere características distintas. Por otro lado, su inmaterialidad lo hacen trasversal a mares y a al espacio aéreo. Aun así, lo verdaderamente distintivo del ciberespacio es el modo en que altera las realidades de los otros tres dominios.

Mientras que los Commons tienen límites definidos de forma más o menos precisa, el ciberespacio es absolutamente trasversal a todos ellos y se solapa con los tres alterando la percepción que se posee de los mismos. El ciberespacio no tiene la misma naturaleza que los demás porque por él discurren realidades que son diferentes de las materiales. La esencia del ciberespacio es básicamente distinta de la de los otros Commons y hace muy difícil su equiparación a ellos.

En la naturaleza se encuentran elementos que actúan a fin de alterar la esencia misma de las cosas que discurren por cualquiera de los otros ámbitos. El entorno marítimo, el aéreo y el terrestre cambian por el mero hecho de que exista el ciberespacio y tenga influencia sobre ellos.

Se tiende a incluir el prefijo ciber a fenómenos que ocurren en el mundo real y se traslada al virtual. En realidad, el ciberespacio supone una alteración del fenómeno en sí y, desde que interactúa con la realidad, la modifica; no para convertirla en una ciber-realidad, sino cambiando su esencia misma dentro del mismo entorno en el que estaba.

Se puede considerar que no existe el ciberataque, existen ataques que se sirven del ciberespacio para producirse. Pero la categorización del ataque no tiene por qué cambiar por el hecho de que se produzca en el ciberespacio o con su ayuda.

[9] Entornos en los que ninguna persona o Estado puede tener su propiedad o control exclusivo y que son básicos para la vida. Contiene un potencial infinito en lo referente al conocimiento y avance de la biología y la sociedad. Incluye los mares, el aire, el espacio y el ciberespacio, en: www.twq.com/10july/docs/10jul_Denmark.pdf. Denmark, Abaham M.: Managing the global Commons.

En realidad, lo que ha cambiado es la naturaleza misma del entorno en el que se producen estas acciones, pues lo que ha cambiado no es la guerra sino el mundo en el que se produce.

A continuación se aproxima al concepto de ciberespacio, identificando aquél como un espacio estratégico para el que hay que definir las medidas de prevención, disuasión, protección y reacción de la ciberdefensa. Identificado como nuevo Global Common, el ciberespacio posee una serie de características diferenciales del resto de los espacios, tales como: [10]

- El ciberespacio es un entorno único, en el que el atacante puede estar en cualquier parte del mundo.
- En la defensa intervienen muchos factores, y no sólo elementos estatales y militares sino también privados. Se exige una estrecha coordinación entre todos ellos.
- La confrontación en el ciberespacio presenta frecuentemente las características de un conflicto asimétrico, y es frecuentemente anónimo y clandestino.
- Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema, y a menudo, sin delatarse.
- Evoluciona rápidamente siguiendo la evolución tecnológica de las tecnologías de la información y la comunicación (TIC).

En ese mismo sentido el Departamento de Defensa de Estados Unidos define al ciberespacio como:

> "Un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores."[11]

En relación al Unión Internacional de Telecomunicaciones (UIT), define al espacio cibernético como, "(…) ciberespacio está integrado por cientos de miles de servidores, ordenadores, conmutadores interconectados y sistemas de transporte de la

[10] Corredera, Casar, José Ramón. *El ciberespacio nuevo escenario de confrontación.* Monografías del CESEDEN 126. Ministerio de Defensa, España, 2012.
[11] Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms.

información (cables, satélites, medios radioeléctricos) que permiten un funcionamiento armonioso de las infraestructuras básicas."[12]

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.

1.2 El ciberespacio como parte del teatro de operaciones

Luego de lograr una interpretación de la naturaleza del espacio cibernético, se buscará en este capítulo expresar la vinculación de la ciberdefensa en el marco del teatro de operaciones.

Si se considera al teatro de operaciones como aquel territorio, tanto propio como enemigo, necesario para el desarrollo de operaciones militares en el nivel operacional[13], en el ciberespacio, las limitaciones geográficas que contienen al teatro de operaciones, desaparecen, ahora "estará conformado por el espacio virtual que ocupa el sistema afectado o que debe ser afectado." [14]

A sí mismo, se entiende que un ataque cibernético puede ser conducido a través de espacios virtuales de la población civil, de empresas, de instituciones o naciones que incluso no saben que están siendo parte de un ciberataque. Esto enfatiza el hecho de que la definición de teatro de operaciones no se aplica en forma taxativa en este nuevo ámbito.

Como se observó en la definición de teatro de guerra, en éste solamente se consideran los espacios terrestres, marítimos y aéreos por lo que el ciberespacio no es aun mencionado implícitamente.

Si se tiene en cuenta que el ciberespacio no tiene fronteras físicas, se considera conveniente, para poder diferenciar los distintos niveles de conducción y a efectos de determinar los alcances de un comando conjunto de ciberdefensa dependiente de un comandante de teatro de operaciones, que sus acciones se centren

[12] Unión Internacional de Telecomunicaciones (UIT). Comisión de Estudio 2-3er Periodo de Estudios (2002-2006) "Informe sobre las infraestructuras nacionales de seguridad del ciberespacio" Ginebra 2006.
[13] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; *Doctrina Básica para la AMC;* PC 00-01, proyecto 2014.
[14] Stel, Enrique. La guerra cibernética el ciberespacio. Editorial Círculo Militar, Buenos Aires, 2005.

en asegurar el comando y control y aquellas otras acciones necesarias para proveerle libertad de acción.

Brett T. Williams señala que la integración de las operaciones en el ciberespacio, las operaciones terrestres, las aeroespaciales y las marítimas son las que alcanzan los objetivos de la campaña[15].

Además indica que independientemente de la naturaleza del ciberespacio que es técnicamente compleja, son el liderazgo y las habilidades de las personas las que aseguren el éxito en las operaciones. Por lo tanto, el ciberespacio, como los otros dominios, requiere oficiales que se han desarrollado a lo largo de sus carreras de un modo que los posicione para liderar en altos niveles de comando y estado mayor.

> *Los oficiales que se especialicen en el ciberespacio debieran pasar sus primeros 10 años de Carrera volviéndose eficientes tácticamente en todos los aspectos de las operaciones en el ciberespacio, capacitarse y completar su educación conjunta, servir en estados mayores conjuntos y comandar en sus áreas de especialidad operacional y completar todas aquellas cosas necesarias para producir generales, comodoros y almirantes cuyo dominio nativo sea el ciberespacio.*[16]

Se puede señalar, que en la doctrina de las Fuerzas Armadas de la República Argentina, el nivel operacional proporciona el enlace crucial entre los objetivos estratégicos y el empleo táctico de las fuerzas del teatro de operaciones. Todas las actividades militares incluidas en un plan de campaña se traducen en un diseño operacional particular[17].

De esta forma, se puede considerar que el ciberespacio es parte del teatro de operaciones (TO), pero se ve a la luz de las definiciones del mismo que no es posible concretar los límites. De esta manera se deberá considerar que todas las acciones cibernéticas que se desarrollan en el TO por parte del enemigo, será absorbida por el comandante del TO como su responsabilidad para rechazarlas.

> *La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la*

---

[15] Brett, Williams T., *"The Joint Force Commander's Guide to Cyberspace Operations"*. Recuperado de: http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/8461/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx.Abril 2015

[16] Ídem.

[17] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la acción militar conjunta nivel operacional*. PC 20-01; Anteproyecto 2014.

"guerra real" y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. Dentro de la amplia gama de operaciones cibernéticas, sólo una porción de éstas afectan específicamente el ámbito de la Defensa Nacional. En efecto, en materia de ciberdefensa existen dificultades fácticas manifiestas para determinar a priori y ab initio si la afectación se trata de una agresión militar estatal externa. Por tal motivo, resulta necesario establecer dicha calificación a posteriori actuando como respuesta inmediata el Sistema de Defensa únicamente en aquellos casos que se persiguieron objetivos bajo protección de dicho sistema, es decir que poseen la intención de alterar e impedir el funcionamiento de sus capacidades.[18]

Ante esta situación, cabe preguntarse cómo será el proceso de toma de decisiones, cómo reaccionará y cómo actuará un comandante operacional para hacerle frente a estos nuevos e incipientes desafíos que se presentan ante las diferentes agencias estatales responsables de la seguridad y defensa nacionales y que plantea este nuevo dominio al que se denominará ciberespacio operacional.

Las Infraestructuras Críticas. Siguiendo dentro del teatro de operaciones, y habiendo explicado al ciberespacio en función de este, existen ciertos aspectos que se deben proteger denominadas "infraestructuras críticas".

Estas se pueden definir como sistemas físicos y sistemas basados en sistemas computacionales complejos que forman parte importante en una sociedad moderna y su funcionamiento fiable y seguro es de suma importancia para la vida económica y la seguridad nacional.[19]

Uno de los elementos del diseño operacional que se vinculan con este tema son, los puntos decisivos a los que se los define como "un conjunto de condiciones o sucesos clave (coordinados en el tiempo y el espacio), tanto para el oponente, propia fuerza o medio ambiente, que deben ser alcanzados a través de efectos y acciones

[18] República Argentina; Decreto 2645/2014; Directiva de Política de Defensa Nacional.
[19] TEN, Chee-Wooi and LIU, Chen-Ching. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. July 2010. Vol. 40, no. 4, p. 853 – 865.

que exploten las vulnerabilidades criticas (VC) y que permitan neutralizar un centro de gravedad (CDG)."[20]

Los PD en materia de ciberdefensa pueden ser, tanto materiales como es el caso de un objetivo físico, sistemas de comando y control del oponente y propio, e incluso puede tratarse de una situación, como podría ser la efectividad de una afectación por un virus informático en la red eléctrica, hídrica o telefónica.

Para ello, se debe establecer claramente el propósito de cada PD con el efecto deseado, este efecto será una acción cibernética sobre una infraestructura crítica, como parte fundamental del plan de campaña.

En lo que respecta al comandante de teatro, este designa como objetivos intermedios los PD que merezcan ser así calificados y asigna recursos para actuar contra ellos.

Se observa como un desafío importante preservar las infraestructuras críticas de la información, garantizar los sistemas de C3IGE (comando, control, comunicaciones, informática y guerra electrónica) de las Fuerzas Armadas, de cualquier acción cibernética enemiga que pudiera afectar el desarrollo de las operaciones militares, teniendo en cuenta que los sistemas informáticos y de comunicación militares deberían ser considerados como una "infraestructura crítica", que posee la particularidad de que los mismos deben estar siempre operables y la información contenida o trasmitida a través de ellos segura, para garantizar eficazmente la defensa de la Nación Argentina y la defensa de nuestros intereses vitales, ante cualquier agresión estatal militar externa.[21]

Es así que estas infraestructuras dentro del TO, recibirán en algún momento de la campaña [22] amenazas, que deberán ser rechazadas (propias) o actuar sobre las del adversario a fin de lograr el objetico operacional.

Las Ciberamenazas. Dentro del espacio cibernético operacional, existen diversas amenazas tales como: troyanos, malware, gusanos, spyware, virus. Cada una posee un nivel de impacto y agresión relacionado directamente con el rol y las funciones

[20] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la acción militar conjunta nivel operacional.* PC 20-01*;* Anteproyecto 2014.
[21] Gastaldi, Sol; *"Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo"*; Informe de Investigación; Escuela de Defensa Nacional, Buenos Aires, 2014.
[22] Serie de operaciones atribuidas a fuerzas de magnitud, que conciben acciones estratégicas, operacionales y tácticas con el mismo propósito, para obtener Objetivos Operacionales y eventualmente Estratégicos, en un tiempo y espacio dados y con ello el logro del Estado Final Operacional.

del objetivo, debiéndose tener en cuenta a la hora de seleccionar el sistema defensivo a emplear en el diseño operacional.

A fin de profundizar en el tema, se puede considerar en un primer momento a las fuentes de ciberataques, como factor a tener en cuenta durante el planeamiento. (Ver Cuadro 1).

Cuadro 1: Fuentes de Ciberataques.[23]

Origen de la amenaza.	Descripción de la amenaza.
Operadores botnets	Son hackers que asumen el control de enormes cantidades de computadoras que emplean para coordinar ataques, basura y sabotajes.
Falsificadores (phishers)	Son grupos que emplean el fraude en un intento de robar identidades o información a fin de obtener beneficios económicos.
Spammer	Son grupos que distribuyen correo electrónico no solicitado, a fin de atacar organizaciones.
Creadores de software espía o malicioso	Son individuos con intenciones de llevar a cabo ataques contra usuarios, produciendo y distribuyendo software espía y malicioso.

Los objetivos primordiales de la ciberataques son las redes más importantes, las que contienen información estratégica. En este sentido, el concepto de ciberguerra va más allá de lo que algunos consideran como simples ataques electrónicos, para incluir a las ya citadas operaciones de información, el hacktivismo, la guerra de redes, la interrupción y negación de la información y/o el ciberterrorismo.[24]

La primera guerra del Golfo Pérsico (1991) se caracterizó por el empleo tanto de ataques convencionales en espacios reales, como por ciberataques en el ciberespacio, mismos que colapsaron las capacidades de comando y control de las fuerzas armadas iraquíes. Como se recordará, la victoria estadounidense –y de sus aliados– fue rápida y aplastante, y en Beijing este hecho fue atribuido a la combinación de estrategias de guerra y ciberguerra, situación considerada como una verdadera revolución en los asuntos militares por la cúpula china.

[23] Fuente: DCAF, Democratic Governance Challenges of Cyber Security, 2009; Geneva.
[24] Charles G. Billo y Welton Chang; *Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States*; Hanover, Institute for Security Technology Studies at Darmouth College, 2004.

Así es que en la mayoría de los actores en los conflictos modernos accionan en algún momento mediante ciberamenazas (Ver Cuadro 2) a fin de contribuir al logro de la destrucción del centro de gravedad.

Cuadro 2: Definición de Ciberamenazas.[25]

Ciberamenaza	Motivación	Dirigido a	Método
Ciberterror	Cambio político/social	Víctimas inocentes	Destrucción a través de las computadoras.
Hacktivismo	Cambio político/social	Tomadores de decisión	Alteración de información o negación de servicio.
Hackeo de sombrero negro	Conflictos en organizaciones	Organizaciones FFAA	Programa maliciosos, virus, gusanos.
Cibercrimen	Beneficios económicos	Organizaciones - FFAA	Programa maliciosos para fraude, robo de identidad. Obtención de información.
Ciberespionaje	Económicos/ Políticos	Organizaciones estatales - FFAA	Empleo de técnicas para operaciones de ataques.
Guerra de Información	Políticos FFAA	Infraestructuras críticas - Sistemas	Empleo de diversas técnicas de ataques.

Se considera en la actualidad que las ciberamenazas siempre van por delante de las medidas que se adoptan. Es así que en años futuros, se espera un incremento del ciberespionaje y el incremento de los ataques como servicio efectuados por grupos con conocimiento y capacidad técnica para realizarlos con garantías de éxito.

Considerando el tema central del trabajo, el conocer las distintas ciberamenazas permite tomar medidas preventivas a fin de proteger las infraestructuras críticas del teatro de operaciones.

Por ello, el comandante en el teatro de operaciones deberá actuar con iniciativa a fin de contar con medidas preventivas en busca de un ciberespacio operacional seguro y confiable.

[25] Fuente: Irving Lachow; *"Cyber Terrorism: Menace or Myth?"* Cyber power and National Security; Washington D.C., Center for Technology and National Security Policy/ National Defense University. 2009.

1.3 Las acciones cibernéticas en el nivel operacional

Durante el tema expuesto anteriormente se ha intentado demostrar el espacio donde se llevarán a cabo acciones cibernéticas, estas serán conducidas por el comandante del TO a fin de apoyar la maniobra operacional en busca del logro del estado final operacional.

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.

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.[26]

Las operaciones militares cibernéticas. La concepción acertada del arte operacional, contribuirá a alcanzar el éxito, y con ello el estado final operacional (EFO). El arte operacional se relaciona con la conducción dentro del teatro de operaciones. En su expresión más simple, determina quién, cuándo, dónde y para qué conducirá las operaciones de las fuerzas que le sean asignadas. El cómo, será responsabilidad de quienes van a llevar a cabo los enfrentamientos en cada plan de operaciones. [27]

En este sentido, durante el proceso de planeamiento en el nivel operacional se considera visualizar como emplear las capacidades disponibles, como así también

[26] Hernández-Ardieta, D. *Capacidades esenciales para una ciberdefensa nacional.* Panamá; Indra 2013.
[27] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la acción militar conjunta nivel operacional.* PC 20-01*;* Anteproyecto 2014.

determinar el enlace entre el empleo táctico de la fuerza y establecer la sincronización de las acciones y los efectos.

De este modo, el nivel operacional determinará efectos cibernéticos a lograr mediante la acción del nivel táctico, a través de la aplicación de las operaciones de ciberdefensa. Entendiendo que estos efectos contribuirán al logro de la maniobra operacional a fin de obtener el estado final operacional.

Se define a la maniobra operacional como la combinación de movimientos y efectos, secuenciales y/o simultáneos desarrollados en un teatro de operaciones, para alcanzar un objetivo operacional, mediante el mejor empleo de los recursos y/o fuerzas disponibles.[28]

Se recuerda que el ciberespacio es considerado como la quinta dimensión del entorno operativo, y de este contexto surge el concepto de operaciones de ciberdefensa, las que lograran el efecto buscado por el comandante operacional.

Las operaciones cibernéticas militares, son aquellas que se desarrollan en el ciberespacio con los mismos objetivos que las que se producen en las dimensiones clásicas del teatro de operaciones: adquirir ventaja, conservarla, situar al enemigo en desventaja y explotarla, las que están compuestas por cuatro componentes:[29]

La ciberoperaciones de red. Deberán permitir el establecimiento, operación, mantenimiento, defensa, mando y control de las redes y sistemas militares; así como de las infraestructuras y recursos críticos.

El cibercombate. Emplea al ciberespacio para causar efectos más allá de las redes y sistemas TIC, permitiendo detectar, disuadir o derrotar a los adversarios. Las capacidades para el cibercombate tendrán como objetivo las redes informáticas y de telecomunicaciones, así como los procesadores, sensores y controladores que se hallan en cualquier equipamiento, sistema, plataforma o infraestructura. El cibercombate podrá emplear tres conjuntos de acciones –ciber-explotación, ciber-ataque y ciber-defensa dinámica – que se ejecutarán de manera coordinada e integrada con las acciones realizadas en los componentes de ciberoperaciones de red y ciberapoyo.

El ciberapoyo. Es un proceso continuo que cubre a los siguientes objetivos: responder, en tiempo y forma, a las necesidades cibernéticas del mando adaptándose

[28] Ídem.
[29] Chamorro, Enrique; *Ciberespacio: La nueva dimensión del entorno operativo.* Documentos de Seguridad y Defensa Nro 44; Centro Superior de Estudios de la Defensa Nacional, España, 2011.

a la continua transformación del ciberespacio global, proporcionando herramientas cibernéticas, ofensivas y defensivas que garanticen la defensa del ciberespacio global de las fuerzas armadas y permitan ejecutar ciberoperaciones; proporcionar al mando nuevos servicios cibernéticos así como evolucionar los servicios ya existentes; garantizar la seguridad del ciberespacio global que se encuentra a disposición de las Fuerzas Armadas minimizando los riesgos, respondiendo eficazmente a los ciber-ataques e intentando anticiparse a futuras acciones de ataque; y conocimiento de la cibersituación.

El conocimiento de la cibersituación. Proporciona el conocimiento inmediato del ciberespacio propio o aliado, el del enemigo y el de cualquier otro de interés, así como el conocimiento del estado y disponibilidad de las capacidades de ciberoperaciones que son necesarias para el planeamiento, conducción y mando y control de las ciberoperaciones y de las operaciones en general.

Si se considera lo expresado, las acciones que se podrán ejecutar son solo aquellas defensivas, teniendo en cuenta que no se podrá ejecutar acciones de ataques cibernéticos en función a las leyes y directivas vigentes en la República Argentina.

En este sentido, el comandante operacional en su diseño deberá considerar efectos cibernéticos a fin de proteger las infraestructuras críticas del TO, materializada por acciones defensivas por parte del nivel táctico.

CAPÍTULO II

La conducción del ciberespacio en el teatro de operaciones

2.1 Los principios de la guerra en el marco de la ciberdefensa

Clausewitz hace una importante distinción entre el fenómeno abstracto de la guerra "ideal" y la práctica de la guerra "real." El primero existe dentro de un marco teórico en el cual el azar, la fricción y la política no tienen ningún impacto durante el choque de armas. Él sostiene que las "leyes de la probabilidad" determinan los altibajos en la guerra real.[30]

Considerado lo expresado, se interpreta que la conducción en el nuevo ambiente operacional debe ser tenido en cuenta en función de las nuevas amenazas existentes. En donde el comandante durante su planeamiento y en la ejecución de las operaciones en materia de ciberdefensa, no deberá descuidar la aplicación de los principios de la guerra.

Estos principios han perdurado a pesar de los cambios de contexto y de la tecnología, los que se definen como aquellos que "(…) se derivan de la experiencia e influencian a la doctrina en todos los niveles. No constituyen una lista de control que garantice el éxito. Sin embargo, si se aplican con recto juicio, proporcionan una guía para el planeamiento y la conducción de las operaciones en todos los niveles."[31]

Si bien los principios de la guerra sirven para contrastar las propias decisiones y las del oponente, su relevancia y aplicación en un momento dado, cambian conforme a las circunstancias. Entendiendo que algunos son considerados durante el planeamiento, mientras otros son guías para la conducción de las operaciones.

Los principios de la guerra para el nivel operacional tenidos en cuenta en el ámbito de la Acción Militar Conjunta son diez: unidad de comando, objetivo, seguridad, sorpresa, ofensiva, concentración, maniobra, moral, sostenimiento, simplicidad y libertad de acción.

A fin de interpretar estos principios, se los definirá conceptualmente para luego vincularlos con aquellos aspectos de relevancia en materia de ciberdefensa.

---

[30] La discusión de Clausewitz con respecto a la guerra "ideal" y "real" está en el Libro Primero en *De La Guerra*. Véase la versión editado y traducido en ingles por Michael Howard y Peter Paret (Princeton, Nueva Jersey: Princeton University Press, 1976), págs. 75-89.

[31] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la acción militar conjunta nivel operacional.* PC 20-01*;* Anteproyecto 2014.

Unidad de Comando (y de esfuerzo). Este principio se refiere a que todas las fuerzas operan bajo un solo comandante con la autoridad requerida para dirigirlas y ser empleadas en alcanzar un propósito común. La finalidad o propósito buscados con este principio es el de asegurar la unidad de esfuerzos bajo un comandante responsable para cada objetivo.[32]

En el nivel operacional, unidad de esfuerzo significa que la acción de los elementos militares de las tres FFAA y agencias civiles involucradas en un teatro de operaciones, debe apuntar al mismo objetivo definido, para asegurar que los esfuerzos se complementen y sean convergentes.

Objetivo. Su propósito es dirigir cada operación militar hacia un objetivo claro, definido, decisivo y alcanzable.

En el nivel operacional, es importante el apoyo mutuo en la obtención del objetivo. Apoyo mutuo significa que la acción conjunta se basa en acciones del ámbito específico de cada Fuerza Armada, que complementan capacidades de las otras, en función del objetivo común buscado.[33]

Seguridad. La aplicación de este principio permitirá evitar o impedir que el enemigo adquiera una ventaja inesperada o sorpresiva. La observancia de este principio es fundamental en un escenario donde la sorpresa es la ventaja fundamental del oponente de cuarta generación.[34]

Poder determinar las distintas amenazas que puede ocasionar un oponente de cuarta generación y estar en condiciones de enfrentarlas exitosamente, permitirá mantener la libertad de acción.

Sorpresa. Su propósito es accionar sobre el oponente en un lugar y momento o en una forma tal, para la que no se encuentre preparado.[35]

La sorpresa en el nivel táctico es más fácil de lograr, que la sorpresa en el nivel operacional o estratégico. La sorpresa implica retener la iniciativa; es una condición previa para el éxito; no el éxito en sí mismo. La sorpresa no necesariamente significa un accionar inesperado, sino que significa que pese a darse cuenta de nuestra acción, el oponente no puede tomar medidas para evitarla.

---

[32] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Manual de Estrategia y Planeamiento para la Acción Militar Conjunta Nivel Operacional – La Campaña.* MC 20 – 01; 2011.

[33] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Manual de Estrategia y Planeamiento para la Acción Militar Conjunta Nivel Operacional – La Campaña.* MC 20 – 01; 2011.

[34] Ídem.

[35] Ídem.

Ofensiva. Este principio permitirá a las fuerzas militares tomar y retener la iniciativa, mientras mantiene la libertad de acción y alcanza resultados decisivos.[36]

Concentración. De acuerdo a la definición dada por el ya citado Manual de Estrategia y Planeamiento, este principio tiene como propósito el de concentrar los efectos del poder de combate en el lugar y tiempo más ventajosos para producir resultados decisivos.[37]

Maniobra. El concepto clásico de maniobra, entendido como una serie de movimientos que tienen como finalidad la de posicionar en forma ventajosa a las propias fuerzas, deja de tener vigencia en este tipo de conflictos caracterizados por la inexistencia de líneas, frentes o dispositivos.[38]

En el nivel operacional reviste importancia la sincronización de la maniobra, que es la coordinación de las acciones militares en tiempo, espacio, oportunidad y propósito, para obtener el máximo poder de combate relativo en el enfrentamiento.

Moral. Su propósito es fomentar el espíritu de cuerpo y la cohesión. La moral es un estado de ánimo individual y colectivo tal, que inspira confianza en el éxito. No debe confundirse el espíritu de cuerpo con el alto estado de ánimo. El primero es permanente, el segundo es transitorio. Una tropa con alta moral es insensible a los vaivenes de la suerte de las armas.[39]

Sostenimiento. Su propósito es sostener a las fuerzas propias durante cada maniobra y fase de la campaña, hasta obtener los objetivos operacionales y el estado final deseado.

En el nivel operacional, el sostenimiento hace a la integración de los esfuerzos para asegurar que no existan organizaciones ni elementos que dupliquen funciones, sino que la clara delimitación en la asignación de responsabilidades permita una integración de esas organizaciones y elementos, sin tener en cuenta el ámbito específico al que pertenezcan.

Simplicidad. Su propósito es preparar planes claros, sin complicaciones y con órdenes concisas que aseguren su comprensión.

La simplicidad contribuye a las operaciones exitosas. Planes sencillos y claros, y órdenes concisas, minimizan las incomprensiones y la confusión.[40]

---

[36] Ministerio de Defensa, op., cit.
[37] Ídem.
[38] Ídem.
[39] Ídem.
[40] Ídem.

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 3).

Cuadro 3: Vinculación de los principios con la ciberdefensa.[41]

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.
Simplicidad	La aplicación de planes simples, contribuyen al éxito de acciones de ciberdefensa exitosas sin confusión y fácil comprensión.

En otro sentido, se puede considerar que la aplicación de los principios guarda una relación directa con el principio militar fundamental (PMF), el que se conoce como un enunciado aplicable al planeamiento de las operaciones militares.

Dicho enunciado expresa que el logro de un objetivo militar (creación o mantenimiento de una situación militar favorable), depende de la ejecución de operaciones eficaces, cuyas características esenciales son: [42]

- Acción eficaz contra objetivos materiales correctos.
- Correcta distribución del poder combativo.
- Proyección de la acción desde posiciones relativas favorables.
- Adecuada libertad de acción.

Dichas características deben cumplir los siguientes requisitos:

- Aptitud, determinada por el factor "efecto deseado".
- Factibilidad, sobre la base del poder relativo.

[41] Fuente: Elaboración personal.
[42] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Estrategia y Planeamiento Nivel Operacional*; MC 20-01, edición 2013.

- Aceptabilidad, determinada por la relación costos-beneficios.

El llamado PMF se aplica en algunos ámbitos geográficos, con mayor énfasis que en otros. En este sentido, se deberá considerar si es aplicable en igual modo en el ciberespacio, al que se lo interpreta como un nuevo ambiente de guerra.

Cabe tener en cuenta que el interrogante que queda planteado, será determinar si la totalidad de los principios mencionados continúan en vigencia para su aplicación en la conducción del ciberespacio militar o deberán ser estudiados e investigado a otros.

De este modo, los actores estatales siguen tratando de encontrar ventajas asimétricas usando el ciberespacio en futuros conflictos mediante operaciones de reunión de inteligencia y ataques ciberespaciales físicos. Por este motivo, se necesita estar preparado tanto para la defensa como para el ataque en el ciberespacio, esto exige y requiere nuevas formas de pensar en la conducción de la campaña.

Por ello, la aplicación de estos principios en el nivel operacional, sumado a otros factores darán como resultante una interoperabilidad conjunta en el teatro de operaciones.

2.2 La interoperabilidad cibernética en el teatro de operaciones

En la búsqueda de una acción conjunta en el teatro de operaciones, el comandante accionará en su conducción aplicando los principios de la guerra, como así también todos aquellos aspectos que logren un accionar mancomunado al logro del objetivo operacional. Uno de estos aspectos y en virtud de la relevancia del tema, surge la necesidad de en un primer momento de entender el significado del concepto de interoperabilidad.

En tal sentido, varios autores han derivado sus afirmaciones en lo que se refiere a la definición de interoperabilidad, entre ellas se puede citar las siguientes:

> "Es la habilidad de los sistemas, unidades o fuerzas para proveer o aceptar servicios de otros sistemas, unidades o fuerzas y para emplear los intercambiados de una forma que permita operar los mismos en forma efectivamente integrada".[43]

[43] FM-101-5-1, *"Operational Terms and Graphics"*, (Department of the Army, Cap. I, pág. 85, edición 1997).

> "Interoperabilidad es la habilidad de sistemas o, unidades para aceptar servicios de otras Fuerzas Armadas o unidades. El uso de los servicios intercambiados les permite operar juntos en forma más efectiva".[44]

De su lectura, surge que este concepto deberá ser asumido por una Fuerza desde la paz, para asegurar la acción conjunta. Esta estandarización no está asociada directamente al planeamiento de estructura de fuerzas, aunque puede tenerse en cuenta para el plan de reequipamiento y adquisiciones. Para poder planear la estructura de fuerzas, se debe contar de antemano con un nivel de estandarización aceptable.

La interoperabilidad es un fenómeno que se registra en todos los niveles de la guerra; comienza a nivel de los Estados Nacionales con la formación de las alianzas con otros países, continua en los niveles operacional y táctico de los teatros de operaciones, con la integración de organizaciones sinérgicas, y finaliza en el nivel técnico con la compatibilidad y estandarización de los equipos desplegados en el terreno.[45]

Como se observa, el concepto de interoperabilidad es amplio y abarcador. Se encuentra fuertemente influido por el concepto sistémico, es decir, el de aunar esfuerzos entre dos o más componentes para lograr un fin. También conlleva la búsqueda de mayor eficacia a menor costo o esfuerzo individual.

No obstante, lo importante es aclarar que muchas veces este concepto se mal interpreta en formar errónea, tales como: 1) hablar un mismo idioma no significa interoperabilidad, sino solamente una condición favorable; 2) mezclar individuos de tropa de diferentes orígenes en una sola fracción orgánica no es interoperabilidad; se intercambian organizaciones y medios, no individuos; el elemento mínimo de integración de tropas es la unidad, porque tiene el espíritu de cuerpo, el conocimiento mutuo de los hombres y el trabajo en equipo requeridos para enfrentar situaciones de alto riesgo que pueden implicar pérdidas de vidas; y 3) que usar el mismo armamento y equipo (salvo los de comunicaciones e informática) no es requisito condicionante de interoperabilidad.[46]

---

[44] FM 100-8, *"The Army in Multinational Operations"*, (Department of the Army, Cap. II, pág. 16, edición 1997).
[45] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Estrategia y Planeamiento Nivel Operacional*; MC 20-01, edición 2013.
[46] Ídem.

El logro de la interoperabilidad en materia de ciberdefensa, guarda una fuerte relación en las características y capacidades de los equipos, los programas informáticos, arquitecturas digitales entre otros, los que estarán equilibrados mediante la conducción del comandante en su aplicación con los principios de la guerra.

La interoperabilidad en el nivel operacional. Esto surge como el resultado de materializar y llevar a la práctica la interoperabilidad estratégica, y principalmente la interoperabilidad estratégica militar. Su concreción resuelve y satisface las necesidades del nivel operacional. Se puede decir, que la interoperabilidad en el nivel operacional es la más difícil de lograr.

La interoperabilidad operacional, entre otros aspectos, incluye el acuerdo y fijación de la estrategia a emplear, los principios militares a observar en el planeamiento común, la compatibilización de las distintas doctrinas de empleo o la aceptación de una de común acuerdo, la negociación y establecimiento de las relaciones de comando, la del consenso en la aceptación e instrumentación de las reglas de empeñamiento en el teatro de operaciones.

Como prueba de que la interoperabilidad operacional es la más dificultosa, se puede mencionar un aspecto relevante: la forma de ejercer el mando. En el que se deberá buscar en todo momento el modo de ejercer el comando, enfatizando la capacidad de control e incrementar la iniciativa y responsabilidad de los subordinados.

Por ello, en la interoperabilidad operacional hay que tener en cuenta: la estructura de comando y control. Esta estructura debe facilitar el proceso de toma de decisiones y el flujo vertical y horizontal de información, pero además debe permitir la unidad de esfuerzos, la dirección centralizada, y la ejecución descentralizada; contar con una doctrina de empleo operacional común; reglas de empeñamiento comunes; una línea de pensamiento común en la toma de decisiones y una estructura de fuerzas y funciones bien definidas.[47]

En este sentido, lo mencionado en relación a la ciberdefensa dentro del nivel operacional, deberá ser tenido en cuenta en todo momento. En un primer momento desde la paz entre las fuerzas en su preparación, como así también el marco legal

[47] Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Estrategia y Planeamiento Nivel Operacional*; MC 20-01, edición 2013.

para la ejecución de las operaciones cibernéticas y aquellos aspectos tecnológicos y de equipamiento que será imprescindible en materia de ciberdefensa.

La interoperabilidad es un fenómeno organizacional permanente, cuya esencia consiste en el establecimiento de una relación sinérgica que tiene lugar tanto entre las partes internas de la estructura de una organización, como entre grupos de ellas desde su creación hasta su fin.

El grado de interoperabilidad cibernética entre dos o más organizaciones no es estático, es dinámico. De ello se deduce que la interoperabilidad no viene con la organización, sino que se desarrolla a fin de atenuar las ciberamenazas en el teatro de operaciones.

Con las condiciones del mundo actual y los adelantos tecnológicos que han reducido los espacios y aumentado las responsabilidades de los Estados, la interoperabilidad cibernética será un requisito indispensable que afectará las infraestructuras críticas de las Fuerzas Armadas de todas las naciones.

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 vinculó el ciberespacio y aquellas acciones que se ejecutan en él, enmarcadas en el teatro de operaciones. Para luego en un segundo capítulo, se analizó a los principios de la guerra en materia cibernética y el concepto de interoperabilidad en función de la conducción en el nivel operacional.

En relación a lo mencionado y luego de haber desarrollado la problemática, surgen finalmente ciertas implicancias y factores en función a la interoperabilidad cibernética operacional.

En este sentido, lo referido al ciberespacio y a las acciones ejecutadas en él, será de carácter difuso en el teatro de operaciones lograr establecer los límites que lo concreten. Es aquí en donde el comandante, deberá identificar para cada fase de la maniobra operacional las infraestructuras críticas a proteger dentro del TO, como así también aquellos efectos cibernéticos a lograr en apoyo a la maniobra operacional, materializados por las acciones de la táctica.

Para ello, se deben ejecutar acciones de ciberdefensa, que permitan el logro de un ciberespacio seguro y confiable. Sumado a esto el contar con una superioridad tecnología, coadyuvará a obtener libertad de acción y el mantenimiento de la iniciativa.

Lo expresado se obtiene mediante 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 ciberamenazas.

Por otra parte, se debe mencionar que es de importancia para el comandante la aplicación de los principios de la guerra en este nivel, tanto durante el planeamiento como en la ejecución de las operaciones.

Es así, como algunos de los principios mencionados se logran vincular con aspectos relacionado con la ciberdefensa, tales como la unidad de comando, la seguridad, la libertad de acción o el objetivo.

Sin embargo se debe considerar en futuras investigaciones, si continuar manteniendo los principios de la guerra doctrinarios u otros principios que guarden relación directa con la ciberdefensa.

Será entonces, contar en la Fuerza con un elemento de ciberdefensa que reúna ciertas características y capacidades, a fin de cumplir con un concepto de empleo operacional, el que se debe destacar por su interoperabilidad conjunta en el TO.

Esta interoperabilidad estará materializada por ser dinámica, con organizaciones flexibles, con medios confiables y de alta compatibilidad. A ello se deberá sumarle, una adecuado Unidad de Comando, que permita una habilidad de sistemas o unidades para aceptar servicios de otras Fuerzas Armadas o unidades a fin de obtener una operación eficiente en el teatro de operaciones.

Los avances tecnológicos junto al elevado nivel de inserción de la cibernética en el nuevo ambiente operacional hacen que un ataque cibernético logre mayores efectos destructivos. Es así como surge la necesidad de identificar en el mercado nacional y regional, tanto civil como militar, herramientas informáticas para el empleo defensivo contra potenciales agresiones cibernéticas.

De esta manera, se debería tener en cuenta avanzar hacia una gestión de las redes informáticas del TO, buscando alcanzar los requisitos mínimos de seguridad para la interoperabilidad de las diferentes Fuerzas, asegurando de manera confiable la defensa homogénea del sistema de información.

BIBLIOGRAFÍA

- Bejarano, José Caro. "El Control de Armas en la Era de la Información". Instituto Español de Estudios Estratégicos Disponible en: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI28a2012_InformationAge_ArmsControl_MJC.pdf. Mayo 2015.
- Carr, Jeffrey. 2011. Inside Cyber Warfare: Mapping the Cyber Underworld. Second Edition. s.l. O´Reilly.
- Cisneros, Ezequiel Rodríguez; *Las operaciones ciberespaciales: desafíos operacionales en el espacio cibernético como nuevo campo de lucha*; Trabajo Final Integrador de la Especialización Estratégica Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta; Buenos Aires; 2012.
- Clarke, Richard A.; Knake, Robert K. 2010. Cyber War: The Next Threat to National Security and What to Do about It. New York. Harpers-Collins Publishers.
- Clausewitz, Karl; *De la Guerra,* Buenos Aires, Editorial Need, 1998, Libro Primero, Cap. I, Pág. 41.
- Corredera, Casar, José Ramón. *El ciberespacio nuevo escenario de confrontación.* Monografías del CESEDEN 126. Ministerio de Defensa, España, 2012.
- Ejército Argentino; *Conducción para las Fuerzas Terrestres*; ROB 00-01, edición 2014.
- Gastaldi, Sol; *"Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo"*; Informe de Investigación; Escuela de Defensa Nacional, Buenos Aires, 2014.
- Giudici, Daniel Eduardo*; La guerra cibernética: lineamientos para la seguridad cibernética en un teatro de operaciones*, Trabajo Final Integrador de la Especialización Estratégica Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta; Buenos Aires; 2013.

- Hernández-Ardieta, D. *Capacidades esenciales para una ciberdefensa nacional*. Panamá; Indra 2013.
- Kuehl, Dan. 2009. From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management. Estados Unidos. College-National Defense University.
- Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Estrategia y Planeamiento Nivel Operacional*; MC 20-01, edición 2013.
- Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; *Planeamiento para la acción militar conjunta nivel operacional*; PC 20-01, edición 2012.
- Ortiz, J. U. Estrategia de Defensa Cibernética en la Era de la Información. *La Revista ESG*. Buenos Aires, Argentina, 2012.
- Palacio, J.; *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, 2013.
- República Argentina; Ministerio de Defensa; "Creación del Comando Conjunto de Ciberdefensa". Resolución MINDEF 343/ 14May14, 2014.
- República Argentina; Ministerio de Defensa; *Libro Blanco de la Defensa*; edición 2010.
- República Argentina; Poder Ejecutivo Nacional; "Directiva de Política de Defensa Nacional". Boletín Oficial Nº 33052, enero de 2015.
- Stel, E. *Guerra Cibernética.* Buenos Aires, Argentina; Círculo Militar, Buenos Aires, 2005.
- Toffler, A. y Toffler, H. 1993. War and AntiWar: Survival at the Dawn of the 21 st Century. Boston. Little Brown and Co.
- Touré, H. *La Búsqueda de la Paz en el Ciberespacio.* Suiza: Unión Internacional de Telecomunicaciones (UIT), 2011.

ANEXO 1: Principales acciones cibernéticas de importancia en el mundo.[48]

Países	Incidente cibernético	Acción de los gobiernos
Alemania	Recibió miles de intentos de espionaje comercial por parte de hackers chinos, que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas. Constantemente recibe ataques por parte de hackers rusos a su red eléctrica y ferroviaria.	Por estos hechos, desde marzo de 2009, estableció su primera unidad exclusivamente dedicada a la guerra cibernética. Esta unidad está conformada por 60 oficiales y suboficiales de todas las fuerzas y está comandada por un general del ejército alemán
Australia	En múltiples ocasiones, hackers norcoreanos y chinos han ingresado y bloqueado páginas web del Gobierno. En noviembre de 2008, el sitio del Primer Ministro fue desconectado completamente por dos días.	De este modo, se creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio. En el Libro Blanco de Defensa de 2009, se definió a la ciberseguridad como una de las capacidades esenciales y principales a fortalecer en los próximos 20 años.
China	Se ha embarcado en una serie de asaltos informáticos a naciones occidentales como Corea del Sur, Alemania, Australia, Reino Unido y Estados Unidos. Tiene una capacidad bien conformada y hombres entrenados dentro del Comando Cibernético Conjunto (militar y civil).	Por ello, ha desarrollado una red operativa muy segura para sus sistemas gubernamentales y militares, haciendo sus redes impenetrables y con un poderío ofensivo que está en posición de demorar o interrumpir el despliegue de tropas de otros países.
Corea del Norte	A pesar de haber sido acusada de numerosos asaltos informáticos, Corea del Norte no ha aceptado oficialmente que dichos asaltos provengan de organismos oficiales.	Tiene operando desde hace aproximadamente 8 años una unidad de guerra cibernética, especializada en hackear las redes militares sur coreanas y norte americanas para extraer información y examinar sus vulnerabilidades.

[48] Fuente: Ministerio de Defensa de Colombia; Recuperado de: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

Corea del Sur	Por su parte, en Corea de Sur sus redes informáticas civiles y militares están bajo continuo ataque; se reporta que mensualmente sufren alrededor de 10.500 intentos de ingresos piratas y de 81.700 contagios con virus informáticos. En 2004, hackers chinos y norcoreanos robaron información ultra secreta de sistemas de diferentes agencias gubernamentales.	En tal sentido, planea la creación de un Comando Conjunto Unificado de Guerra Cibernética para 2012 con el fin de enfrentar la amenaza creciente de ataques a sus redes informáticas gubernamentales y militares. Las entidades civiles han desarrollado un fuerte mecanismo privado de defensa a los ataques, dada la poca eficiencia de las acciones adelantadas en este sentido por parte del Estado.
Estados Unidos	Durante enero de 2009, hackers robaron información ultra secreta del Joint Strike Fighter o F-35 (el proyecto de un sistema de armas más costoso en la historia de Estados Unidos). El 4 de julio de 2009, deshabilitaron las páginas web del Departamento del Tesoro y de Estado, de la Comisión Federal de Comercio, del Pentágono y de la Casa Blanca.	Se creó un Centro de Ciber Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés). Este Centro optimiza los esfuerzos hechos por parte de las Fuerzas Militares y otras agencias, y provee al país con la capacidad de defender la infraestructura tecnológica y de conducir operaciones ofensivas.
Estonia	En 2007, Estonia sufrió el peor ataque cibernético ocurrido en la historia. Luego de un incidente diplomático, hackers rusos bloquearon los sistemas informáticos de las agencias gubernamentales. El país quedó completamente desconectado y sin servicios bancarios, de internet y de fluido eléctrico por varios días.	En función a lo sucedido, en 2008 creó conjuntamente con varios países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciberamenazas. En este centro trabajan 30 personas, entre personal técnico y administrativo. Su presupuesto proviene de los países participantes de manera compartida.
Francia	Durante enero de 2009, aviones de combate franceses no pudieron despegar de su portaviones al ser desactivado, por medio de un virus	Así es como creó la Agencia de Seguridad para las Redes e Información (FINSA), que vigila las redes informáticas

	informático, su sistema electrónico.	gubernamentales y privadas con el fin de defender las de ataques cibernéticos. Esta agencia depende directamente del Ministro de Seguridad Nacional. Francia lidera la Unidad de Ciberseguridad y Ciberdefensa en la OTAN.