IUE

Instituto Universitario del Ejército

Instituto Universitario Art. 77 – Ley 24.521

Escuela Superior de Guerra

"Tte Grl Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "La estrategia de Argentina y Brasil para la Defensa Cibernética, una análisis por los niveles de la conducción"

Que para acceder al título de Especialista en Conducción Superior de OOMMTT, presenta el Mayor Don VICTOR JOSÉ QUEIROZ CABRAL.

Ciudad Autónoma de Buenos Aires, 16 de octubre de 2015.

Agradecimiento

En primer lugar gracias a Dios por darme la oportunidad de completar este trabajo y el Curso de Estado Mayor de la Escuela de Guerra del Ejército Argentino.

También, agradezco a mis padres por haberme proporcionado educación para llegar a donde estoy. Todo lo que tengo es porque ustedes siempre me enseñaron a buscar.

Mis hijas, simplemente, por existir en mi vida.

El Ejército Argentino por las lecciones aprendidas durante este año.

Los nuevos amigos de COEM/2015 por la amistad que seguramente continuará en los próximos años.

Listado de Abreviaturas

1º BGE	- 1º Batallón de Guerra Electrónica
ABIN	- Agencia Brasileña de Inteligencia
AFIP	- Administración Federal de Ingresos Públicos
ANATEL	- Agencia Nacional de Telecomunicaciones
CCDCEO	- Centro de Excelencia Cooperativa de Ciberdefensa
CDCiber	- Centro Cibernético de Defensa del Ejército
CDN	- Consejo de Defensa Nacional
CEPESC	- Centro de Investigación y Desarrollo de Seguridad de Comunicaciones
CGI.br	- Comité Gestor de la Internet en Brasil
Cia GE	- Compañía de Guerra Electrónica
Cia Mon Ciber	- Monitoreo y Guerra Cibernética
CIGE	- Centro de Enseñanza de Guerra Electrónica
CREDEN	- Cámara de Relaciones Exteriores y Defensa Nacional
DoS	- *Denial of Service*
DPF	- Departamento da Policía Federal
DSIC	- Departamento de Seguridad de Información y Comunicación
Dst Cj Def Ciber	- Destacamento Conjunto de Defensa Cibernética
Dst Cj G Ciber	- Destacamento Conjunto de Guerra Cibernética
EA	- Ejército Argentino
EB	- Ejército Brasileño
EEUU	- Estados Unidos
EMCFA	- Estado Mayor Conjunto de las Fuerzas Armadas - Brasil
EMCFFAA	- Estado Mayor Conjunto de las Fuerzas Armadas - Argentina
END	- Estrategia Nacional de Defensa
FFAA	- Fuerzas Armadas
GSI/PR	- Gabinete de Seguridad Institucional de Brasil
ICIC	- Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad
MD	- Ministerio de la Defensa
ONTI	- Oficina Nacional de Tecnologías de Información
ONU	- Organización de las Naciones Unidas
OTAN	- Organización del Tratado de Atlántico Norte
PBC	- Planeamiento Basada en Capacidades
PEN	- Planeamiento Estratégico Nacional
SERPRO	- Servicio Federal de Procesamiento de Datos
SISBIN	- Sistema Brasileño de Inteligencia
SMDC	- Sistema Militar de Defensa Cibernética
SQL	- *Structured Query Language*
TIC	- Tecnología Información y Comunicaciones
UNASUL	- Unión de las Naciones Sudamericanas
VLS	- Vehículo de Lanzamiento Satélite

Listado de Figuras

Índice de Contenido

Resumen

El trabajo es una apreciación sobre las estrategias de Argentina y Brasil para emplear las nuevas tecnologías venidas por la revolución de la expansión cibernética. Estos nuevos conceptos trajeron también riesgos y desafíos para la Defensa Nacional. Así, los países buscan la mejor forma de combatir dentro del Espacio Cibernético. Argentina y Brasil siguen la tendencia mundial de proteger sus infraestructuras críticas contra estas nuevas amenazas, pasando a ser una responsabilidad de la Defensa Nacional y por la coordinación de las Fuerzas Armadas. Por lo tanto, la mayor dificultad es coordinar los esfuerzos de la Nación para alcanzar los objetivos nacionales. Los Niveles de la Conducción son fundamentales para la gestión de estos riesgos. Este trabajo presenta como Argentina y Brasil planearon el desarrollo de sus Sectores Cibernéticos. La opción argentina fue primer firmar los marcos legales, para después conformar un Centro Conjunto de Defensa Cibernética como centro de estudios e acciones en el Sector. Cuanto Brasil, la Estrategia Nacional de Defensa de año 2008 es el principal marco legal para inicio de las actividades bajo la coordinación del Ejército Brasileño. El Centro de Defensa Cibernético del Ejército ya tuvo algunas experiencias de empleo operacional gracias a los gran eventos que el País estuve de anfitrión en los últimos años, que validaron una nueva Doctrina Cibernética de Defensa, con estructuras flexibles y modulares, como los Destacamentos Conjunto de Defensa Cibernética y Destacamento Conjunto de Guerra Cibernética. Ambos los países tienen puntos en comunes y algunas distinciones, conservando las idiosincrasias de cada país.

Palabras claves: 1. Cibernética 2. Niveles de la Conducción 3. Ejército Argentino 4. Ejército Brasileño

Introducción

Antecedentes y justificación del problema

Nunca antes en la historia de la humanidad el conflicto sufriera tantas evoluciones en la forma de combatir. En la actualidad, el ambiente operativo se tornó complejo, gracias el resultado de un gran desarrollo tecnológico, la facilidad en acceso a los medios de alta tecnología y los cambios de comportamiento del hombre moderno.

La complejidad del campo de batalla actual tiene distintas características, entre ellas está el desarrollo de un ambiente cibernético fundamental en la búsqueda de información y del dominio de las acciones ante el oponente.

Sintonizado con estas nuevas características, el Ejército Argentino (EA) actualizó su Reglamento de Conducción para las Fuerzas Terrestres, ROB-00-01, año 2014, que presenta el espacio cibernético como una de las características de una mayor complejidad operacional (EJÉRCITO ARGENTINO, 2014, p. 1-13)[1].

El concepto ya establecido de la "Era de la Información", también conocido por muchos autores como "Era Digital" o "Era del Conocimiento", tiene como concepto clave la gran capacidad de almacenar, procesar y transmitir informaciones y conocimientos. Por lo tanto, el ciberespacio se ha convertido en la frontera y el ambiente de explotación y transmisión de datos. En el mundo actual, estas grandes facilidades y ventajas vinos de la informática y la Internet también aumentó la vulnerabilidad de los sistemas.

Hoy en día podemos decir que la economía mundial se ha hecho dependiente de ciberespacio[2]. El sistema bancario y financiero en todo el mundo es un ejemplo de esa dependencia, que van desde sistemas informáticos complejos de grandes grupos empresariales a un *smartphone*[3] sencillo de un ciudadano común.

[1] La edición anterior del ROB 00-01 es de 1997 y no contempla los conceptos de la guerra en ciberespacio.
[2] Ciberespacio – terminología empleada por los expertos, referente a espacio cibernético.
[3] Smartphone – terminología empleada para teléfonos celulares con tecnología de transmisión de datos.

El Diario Clarin (2015), presenta dátalos que confirman la dependencia mundial debajo de la internet. 2,9 billones de personas, 40% de la población mundial, y 6,8 billones de dispositivos (entre PCs, smartphones, servidores, etc) están unidos a web; se envían 204 millones de e-mail por minutos y en la Argentina 22 millones de usuarios con un promedio de 5 horas por día.

Con base en la observación de estos acontecimientos, los Estados están evolucionando sus estrategias para alcanzar el logro de sus objetivos nacionales. Así, se convirtió casi en un tema vital para proteger sus sistemas y estructuras críticas conformadas en un ambiente cibernético.

El ciberespacio pasó a ser explorado dentro del espectro del conflicto. La Guerra Asimétrica, entre los actores estatales o no, aprovechó las debilidades generadas por la creciente dependencia cibernética para alcanzar los objetivos inalcanzables por medio del combate convencional u abierta. Una sola persona, no necesariamente experto en el Arte de la Guerra, puede llevar al caos un Estado Soberano o, simplemente, causar daños irreparables a la estructura de su gobierno o de su población.

Por lo tanto, la amenaza cibernética ha despertado interés en el tema de la Defensa Nacional en todas las Fuerzas Armadas (FFAA) del Mundo. De este modo, tanto Brasil como Argentina ha estado estudiando el tema y desarrollando sus proyectos de defensa cibernética. Pero, después de los primeros años de estudio por sus Fuerzas Armadas, es posible llegar a las primeras conclusiones, y que el tema abarca mucho más que los militares, sino también diversos segmentos de los Gobierno, cambiando el problema para además de los militares, más también para toda la sociedad.

Los Estados Unidos (EEUU), reconocida por varios expertos como la más grande potencia militar del Mundo, ha estado trabajando este tema en la última década, y es el principal difusor de conceptos militares dentro del ciberespacio.

Así, la integración de los conceptos con otras capacidades en beneficio de las operaciones militares, previsto en reglamento estadunidense FM 3-38, *Ciber Electomagnetic Activities,* (Ejército del EEUU, 2014, p. 1-2)[4] sirven como fuente de inspiración para esta obra.

El trabajo es un análisis de las trayectorias seguidas por Argentina y Brasil para complementar sus estrategias de implementación de Defensa Cibernética. Al final, después de los primeros pasos en éste campo, se puede hacer una análisis entre la estructura del Sector Cibernético de ambos países, buscando identificar oportunidades de mejora y desarrollo sinérgico conjunto, sin embargo apuntar ninguna crítica a la conducción de estos países. Además, este trabajo se presenta el punto de vista del autor, y no lo es una opinión institucional de los países.

A pesar de la divulgación de los primeros marcos teóricos sobre el tema, todavía el asunto está lleno de dudas y blancos, considerado nuevo en el campo de las ciencias militares, como también por las incertidumbres derivadas de los escenarios de los conflictos actuales.

Por último, esta analice no agota el tema. Sirve como motivación para nuevos estudios sean más complejos y profundos.

Planteo del problema

El problema surge de las grandes incertidumbres sobre la forma de conducir el combate en ciberespacio. Es un problema que atraviesa todos los Ejércitos del Mundo.

Dada su amplitud del tema, los marcos teóricos argentinos y brasileños aún son vagos, y no tratan como desarrollar de una forma práctica las acciones cibernéticas. Se

[4] *Ciber Electomagnetic Activities* - terminología empleada en la doctrina del EEUU que concentra actividades de Guerra Electrónica, Guerra Cibernética y Administración del Espectro electromagnético.

quedan apenas en nivel estratégico conceptual. Seguramente, el futuro profundamente del tema facilitará estos países a desarrollar cada vez más sus "*modos de acción*".

Ante esta situación, el problema de estudio se guiará por la siguiente pregunta:

Considerando o ambiente operacional actual, ¿Cuáles serían las mejores organizaciones para conducir y emplear el Sector Cibernético en los Ejércitos de Argentina y Brasil?

La investigación está delimitada por las leyes y reglamentos doctrinarios actuales de las FFAA de Argentina y Brasil. Todavía, para apoyo conceptual serán utilizados el reglamento estadunidense FM 3-38, *Ciber Electomagnetic Activities,* y también en la literatura de expertos sobre el tema.

Objetivos de la investigación

Objetivo general. Analizar la estrategia de conducción y empleo de Defensa Cibernética de Argentina y Brasil, de acuerdo a los niveles de la conducción.

Objetivos específicos. Para desarrollo del trabajo fueron elegidos tres objetivos específicos listados abajo:

- Conocer, descreer y la doctrina básica de empleo de Defesa Cibernética aceptos por Argentina y Brasil

- Describir la estructura necesaria del Sector Cibernético en Nivel Estratégico Nacional y Estratégico Militar

- Describir la estructura necesaria del Sector Cibernético en Nivel Operacional y Táctico

Aspectos sobresalientes del marco teórico

La analice tuve como base la revisión de los documentos escritos sobre el tema. En primer lugar, el estudio de los documentos oficiales, tales como leyes, decretos y reglamentos de Gobiernos y de las FFAA de Argentina y Brasil fueron vitales para la investigación. Después, se consideró la literatura técnica laborada por diversos autores sobre el tema. Así, en seguida, se buscó una apreciación comparativa de la doctrina del Ejército de los EEUU, como auxilio para validar los conceptos y estructuras establecidas. Por último, los modelos de Argentina y Brasil fueron analizados sin dar una valoración de los aspectos positivos o negativos de las estructuras adoptadas.

En Brasil, en un principio, el proceso fue establecido por el Decreto Presidencial Nº 6.703, aprobada el 18 de diciembre de 2008, que aprobó la Estrategia Nacional de Defensa (END). En este documento, se estableció que el Ejército Brasileño sería el organismo encargado de la conducción y desarrollo de las actividades del Sector. Más tarde, ha seguido la jerarquía legal de Brasil, una serie de documentos fueron hechos para promover el empleo efectivo del Sector Cibernético por las FFAA, siempre en un ambiente de amplio espectro y amenazas difusas.

Por lo tanto, se estableció como el principal marco teórico los principales documentos de Brasil y Argentina sobre el tema, tales como:

- **Brasil**: Política Cibernética de Defesa, hecha en año 2012; y la, Doctrina Militar de Defensa Cibernética, hecha en año 2014.
- **Argentina**: Resolución JGM Nº 580/2011 que establece la creación del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.
- **EEUU**: FM 3-38, *Ciber Electomagnetic Activities,* 2014.
- Otros reglamentos de Argentina y Brasil que fueron analizados, tanto hechos por la Administración Federal cuanto por las FFAA.

- Además, fueron utilizadas como fuente de investigación, las diversas literaturas civiles y militares específicas del tema.

Metodología empleada

La Investigación se cuantificó por la subjetividad y la experiencia del autor, a través del análisis de documentos sin una medición estadística de los datos estudiados. Tuvo una finalidad descriptiva, por poder comprobar características y relaciones entre los resultados obtenidos. Puso considerarla también una investigación explicativa, por poder aclarar factos concretos ocurridos de ciertos fenómenos.

Con respecto a los medios de investigación, la investigación se clasificó como bibliográfica y documental, por todavía se basó en los exámenes de obras literarias de autores expertos, así como documentación interna y oficial, como Decretos, Reglamentos y varios periódicos, argentinos y brasileños.

En este trabajo se presenta el método deductivo y comparativo y busca desafiar el problema sugerido por una comparación de las estructuras adoptadas por Argentina y Brasil, presentando sus similitudes y diferencias.

Relevancia de la investigación

La humanidad pasó solamente apenas dos veces por un cambio tan significativo como la actual "Era del Conocimiento". La primera vez se dio hay cerca de 10 mil años, cuando la especie humana pasó de civilización eminentemente nómade para civilización sedentaria, a partir del dominio de las tecnologías agrícolas. La segunda vez, cerca de 330 años, cuando la especie humana dejo de ser una civilización predominantemente agrícola y torno se una civilización industrial, por dominar nuevas tecnologías de fabricación de bienes de consumo, en especial las máquinas a vapor. (TOFFLER, p. 55).

Utilizar el espacio cibernético es una forma de ampliar el poder militar de un país, necesariamente, una novedad. Otros países con elevado poder militar cómo los EEUU, Rusia y China ya poseen sus Centros o Comandos Cibernéticos. Esta es una tendencia de todos los ejércitos del Mundo. Sin embargo, cada Nación desarrolla la mejor manera de la emplear en su provecho, considerando sus propias peculiaridades.

CAPITULO I

La estrategia de Argentina para Defensa Cibernética

Finalidad del Capítulo

La Guerra Cibernética es llamada de forma genérica para las FFAA argentinas apenas como Defensa Cibernética, conservando todas las características de los dos términos. Tiene por naturaleza ser asimétrica, aumentando la vulnerabilidad de los actores que más dependen del apoyo la Tecnología Información y Comunicaciones (TIC), como los países desarrollados. Así cuando el asunto es Defensa Nacional hay una nivelación inevitable entre fuerte y débil.

La intención principal de este capítulo es presentar el desarrollo de la Defensa Cibernética en la Argentina de su origen hasta el estadio actual. El caso argentino, la presentación de algunos conceptos son fundamentales, principalmente por la clara aducción de pensamiento que separa "**Seguridad**" y "**Defensa**". La lógica es considerar el Estado Nacional como soberano dentro de sus límites, no aceptando acciones que pongan en riesgos la Defesa Nacional dentro de su perímetro. Esta óptica, las acciones de seguridad interna jamás serán de responsabilidad de las Fuerzas Armadas. Esta débil separación no es clara en los demás países de la Sudamérica, como en el caso brasileño, estudiado en el Capítulo II.

Estés conceptos son importantes dentro del estudio de la cibernética, por la dificultad de identificación del agente responsable por la amenaza virtual, sus "reales" intenciones. Ejemplo: Uno ataque deliberado, no identificado, a una red de datos de un Banco Estatal es un tema de Seguridad Pública? Probablemente, sí. Pero, lo que difiere de una invasión de rede realizada por uno ladrón común de claves bancarias de uno ataque cibernético de terroristas o de fuerzas cibernéticas especializadas de un país agresor? Las respuestas no

son fáciles. El punto clave da cuestión se queda no en las acciones, más en los efectos que se desea alcanzar. No caso cibernético, estés efectos no son tan fáciles identificación.

Así, el Teniente Coronel de Infantería Roberto Uzal (2012, p. 40 y 42), del Ejército Argentino (EA), en su artigo sobre los desafíos más relevantes para la Defensa Nacional argentina, auxilia en definición de los conceptos de crimen cibernético, terrorismo cibernético o guerra cibernética. **Crimen Cibernético** es el acto criminal cometido mediante la utilización de computadoras como herramientas principales para cometer el delito. Suele también generalizarse que existe crimen cibernético si computadores han sido objeto, sujeto o instrumento del ilícito. La definición de **Terrorismo Cibernético o Ciberterrorismo** puede ser resumida como Crimen Cibernético pero realizado por motivaciones religiosas, sociales o políticas.

El mismo autor presenta la definición de según Jeffrey Carr, autor de "*Inside Cyber Warfare*", en la cual sólo hay **Guerra Cibernética** en acciones de Estado contra otro Estado. Confundir Guerra Cibernética con Crimen Cibernético, por ejemplo, es un grave error conceptual.

Existen aún una infinidad de otros conceptos también relacionados al tema cibernética. Pero, es fundamental entender su ambiente operacional y los desafíos del mundo actual.

El concepto más amplio y base estratégica para cualquier Estado es de **Seguridad de la Información**. No por eso, saber se proteger es el punto inicial de la estrategia de cualquier Estado. El modelo argentino, este concepto es fundamental por su adopción por la estrategia defensiva. El control de esa información en "ciberespacio" puede ser clasificado como Seguridad Informática, o virtual.

Con estas premisas, es posible interpretar el concepto de **ciberdefensa**, como siendo la seguridad de esa información que camina involucrada en este ciberespacio aplicada a

Defesa Nacional. Tiene la principal finalidad de planear, coordinar, integrar, sincronizar, conducir e ejecutar actividades relacionadas a la protección de las redes de computadores de la área de Defesa, como también, aquellas acciones cibernéticas provenientes de otras naciones que comprometan las estructuras críticas del País y sus servicios esenciales (7º Simposio Argentino de Informática de Estado, 2013, p. 281)[5].

La definición presentada por Hernandez (2013, p. 04) de la Empresa de Tecnología INDRA, complementa la definición arriba, informando que estés sistemas críticos pueden ser extendidos a sistemas civiles. De un punto de vista práctico, la mayoría de los sistemas de ciberdefensa proveen de sistemas de ciberseguridad ampliamente probados y adoptados por las estructuras militares.

El Profesor en Derecho de la Universidad de Temple, EEUU, Duncan Hollis, presenta la preocupación mundial sobre la diferenciación de crimines cibernéticos de ataques cibernéticos. Para la doctrina estadunidense los ataques podrán ser considerados actos de guerra. Lo que legitima una acción de fuerzas militares convencionales. Entonces, debajo de una agresión, según las leyes internacionales, él país tiene derecho de defenderse y no solo a través de la informática (Gee, 2009, p.37). Así también, defiende la OTAN en el Centro de Excelencia Cooperativa de Ciberdefensa (CCDCEO, sigla en ingles)[6], ubicado en Talinn, Estonia, cuya la posición pasa por la Carta de la ONU en su artigo 51.

El 7º Sétimo Simposio Argentino de Estado, Uzel (2013, p. 282) [7] hizo consideraciones sobre el peligro de confundir la Guerra Cibernética con la Guerra Electrónica, la primera se ocupa de la información dentro del ciberespacio, mientras el segundo dentro del dominio del espectro electromagnético.

Posteriormente, en 2014, la doctrina del Ejército de los EEUU confirman que existe una área gris de intersección entre Guerra Cibernética (CO, de la sigla en inglés,

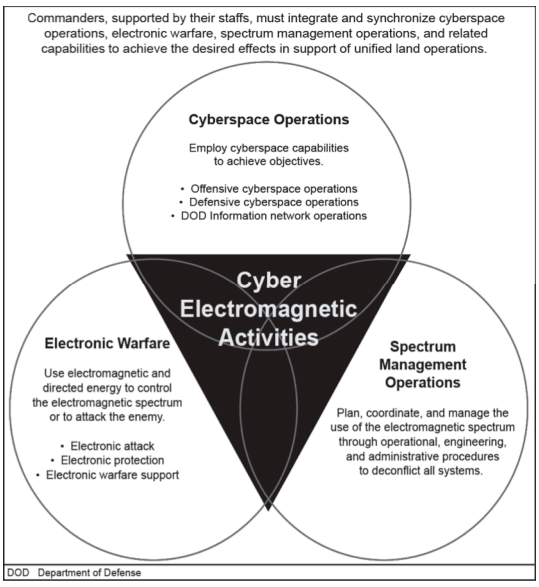
[5] 7º Simposio Argentino de Informática de Estado (2013) p.281.
[6] OTAN – en ingles, NATO. *Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/
[7] 7º Simposio Argentino de Informática de Estado (2013) p.282.

cyberspace operations) y Guerra Electrónica (EW, de la sigla en inglés, *electronic warfare*). Así, lo definió un nuevo concepto que originó el reglamento estadunidense, FM 3-38*, cyber electromagnetic activities.*

Este nuevo concepto significa las actividades realizadas para explotar y mantener una ventaja sobre adversarios, tanto en el ciberespacio cuanto en el espectro electromagnético, mientras también, negar el enemigo el empleo de los sistemas de comando y control. Esta nueva actividad aun contempla operaciones de gerenciamiento y control de lo espectro, conforme figura abajo (Ejército de EEUU, FM 3-38, p.1-1).

Los estadunidenses presentaran este nuevo concepto gracias, principalmente, al adviento de modernos equipamientos de GE con capacidades cibernéticas que tienen como blanco tirar provecto de redes *wi-fi* o *bluetooth*.

Figura 1 – Área de actuación de la cybe eletrocmagnetic activities



Fuente – FM 3-38 Cybe Eletrocmagnetic activities

Antecedentes y marcos legales argentinos

El Estado Argentino, en especial sus FFAA, vienen acompañando la revolución tecnológica que impulsó la cibernética en mundo actual. Diversos son los estudios y ejemplos sobre el tema en el mundo. A dependencia de sistemas digitales es una realidad para todos los Estados. Sin embargo, un acto sirvió de alerta para el Estado Argentino. En 2010, el sitio web de la Administración Federal de Ingresos Públicos (AFIP), generó una error en los datos personales de contribuyentes, demostrando grande vulnerabilidad das redes gubernamentales. Se quedó confirmado que los sistemas de información del Gobierno necesitaban de seguranza (CANDELA, SOL, FERNANDÉZ, 2014, p.1).

El marco inicial para a ciberdefensa argentina viene de la Ley de Defesa Nacional Nº 23.554/88 (Poder Legislativo Nacional, 1988), donde se identifica las amenazas externas y agresiones de otros Estados como criterio fundamental para empleo del Instrumento Militar.

Ese concepto arriba fue aclarado y mejor definido en el Decreto Regulador Nº 727/06 (Poder Executivo Nacional, 2006), que dispone: “se entenderá como 'agresión de origen externo' el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país”.

Por su parte, el Decreto Nº 1.691/06 (Poder Ejecutivo Nacional, 2006), Directiva de Organización y Funcionamiento de las Fuerzas Armadas, presenta que las FFAA deben organizar con base en su principal empleo constitucional, o sea, la defensa de la Patria contra una agresión externa.

La Ley Nº 24.948/98 (Poder Legislativo Nacional, 1998), de reestructuración de las FFAA, reconocen el empleo del Instrumento Militar para las operaciones subsidiarias. Este marco legal, allá de ampliar la participación de las FFAA como órgano de apoyo a seguridad interior, posibilita su participación en la construcción de un Sistema de Defesa

Subregional, abriendo la posibilidad de colaboración e integración con los vecinos del entorno estratégico, como Brasil.

Por fin, dentro del marco legal, el Decreto 1.714/09 (Poder Executivo Nacional, 2009), que aprobó la Política de Defesa Nacional, presenta la adopción del modelo argentino de características defensivas, pautado en la legítima defensa frente una agresión de Estados extranjeros.

En nivel de Poder Executivo, el Gobierno inició su estrategia cibernética en sentido "*up-down*", o sea, de arriba para bajo, de los niveles más altos para los más bajos. Pretende implementar todo un sistema de gestión de Seguridad de la Información, desde el nivel Estratégico Nacional hasta el Táctico.

El Libro Blanco de Defensa Nacional resalta el interés estratégico por dominio del ciberespacio para o ejercicio del comando y control, y funcionamiento de las redes de sistemas de defensa. Este marco, se queda claro la participación de las FFAA como actor participativo del servicio nacional de alerta estratégico de amenazas cibernéticas.

Una de la primeras medidas fue la edición de la Resolución Nº 580/2011 (Poder Executivo Nacional, 2011) que creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)[8] bajo de la Oficina Nacional de Tecnologías de Información (ONTI) subordinada a Subsecretaria de Tecnologías de Gestión de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros. Este programa visa apreciar y proponer la implementación de los marcos regulatorios necesarios a identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional y las organizaciones privadas de interés estatal, cómo también adoptar estrategias o estructuras para desarrollo de tecnologías.

[8] Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad ICIC- Recuperado: http://www.icic.gob.ar/

Dentro del programa arriba citado, por medio de la Disposición Nr 2/2013 de la ONTI, fueron criados los Grupos de Trabajo de especialistas en las prioridades establecidas por la Oficina:

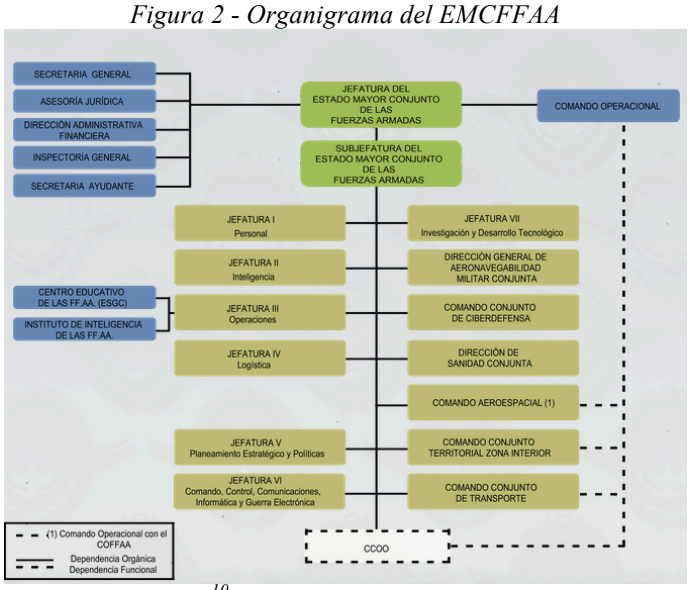
- ICIC-CERT (*Computer Emergency Response Team*): tiene la tarea de administrar la información, centralizar los reportes y realizar el asesoramiento técnico.
- ICIC- GAP (Grupo de Acción Preventiva): Grupo dedicado la pesquisa y prospección, con la finalidad de investigar e incorporar nuevas tecnologías.
- ICIC-GICI (Grupo de Infraestructuras Críticas e Información): Visa establecer prioridades y planos estratégicos para ciberseguridad, en colaboración con el sector privado.
- ICIC-Internet SANO: promover la concientización del risco advenido del mundo digital.

Gracias al trabajo realizado por la ONTI, fue aprobada la Política Modelo de Seguridad de Información[9], a través de la Disposición Nº 1/2015. Se trata de un documento completo con una definición política y organización de Seguridad de la Información, cómo también los riesgos y amenazas para el Estado Argentino.

Dentro de las FFAA, el Estado Mayor Conjunto de las Fuerzas Armadas (EMCFFAA) tiene establecido por medio de la Resolución Nº 343/MD, de 14 de mayo de 2014, el Comando de Conjunto de Ciberdefensa, como conductor de las acciones de Seguridad de la Información y Comunicaciones en la Defensa Nacional.

[9] Política Modelo de Seguridad da Información. Recuperado: http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Figura 2 - Organigrama del EMCFFAA



Fuente - EMCFFAA[10]

El Decreto Nº 378/05 (Poder Executivo Nacional, 2005), versa sobre el Planeamiento Estratégico Nacional (PEN) aprobó el Lineamiento Estratégico del Plan Nacional de Gobierno Electrónico y los Planes Sectoriales de Gobierno Electrónicos para la promoción y empleo eficiente y coordinado de los recursos de TIC.

Por lo tanto, en 2015 fue realizada la Tercera Edición del Ejercicio Nacional de Respuestas de Incidentes Cibernéticos en el Destruidor Almirante Brown. En la oportunidad el Vicealmirante Marcelo Eduardo Hipólito Srurs declaró que la colaboración del ICIC es un logro estratégico del Ministerio de la Defensa (LUCERO, 2015, p.41).

Dentro del Ejército Argentino y en consecuencia de la creación del Comando Conjunto Cibernético, fue creado en día 14 de Noviembre de 2014, el Centro Cibernético del Ejército subordinado al Jefe de Estado Mayor General del Ejército y con enlaces logísticos con la Dirección General de Inteligencia. Este Centro tiene la función de monitorear permanentemente las Infraestructuras Críticas de Información de Ejército, y sus sistemas y servicios asociados, con la finalidad de brindar respuestas a los incidentes de informática y proteger los activos que le compete.

[10] EMCFFAA Recuperado: http://www.fuerzas-armadas.mil.ar/Organigrama.aspx

Afora del territorio argentino, dentro de la Unión de las Naciones Sudamericanas (UNASUL), se destaca la Declaración de Buenos Aires, una declaración conjunta entre los Ministros de la Defesa de Argentina y Brasil, en que deciden conformar un grupo de trabajo para desarrollo conjunto de métodos, sistemas tecnológicos, doctrina combinada, investigación científica, intercambio de experiencias para incrementar la seguridad de la información.

La Defensa Cibernética en Ejército Argentino

La doctrina adoptada por EA divide los niveles de la conducción en niveles. Pero con una separación didáctica entre el nivel estratégico, entre Estratégico General (o Nacional, o Gran Estrategia) y Estratégico Militar. Esta división visa sólo separar todos los medios relacionados al Poder Nacional, con aquellos relacionados a Estrategia Militar.

Abajo sigue una figura presentada en reglamento ROB 00-01, Conducción de las Fuerzas Terrestres del EA.

Figura 3– Relaciones entre los Niveles de la Guerra, los Niveles de la Conducción, recursos y finalidades

NIVELES DE GUERRA	NIVELES DE CONDUCCIÓN	RECURSOS	FINALIDAD
ESTRATÉGICO	Estratégico general o nacional o Gran Estrategia.	Todos los medios del Poder Nacional.	El estado final político.
	Estratégico militar.	Todos los medios ilitares del Poder Nacional y, eventualmente, aquellos otros provenientes del Poder Nacional.	El estado final militar.
OPERACIONAL	Operacional.	Los asignados a los comandantes de nivel operacinal.	El estado final operacional.
TÁCTICO	Táctico.	Los medios que se emplean en una operación militar.	Obtener los puntos decisivos y los objetivos de acuerdo con el plan de campaña.

Cuadro Nro 1-III Relaciones entre los Niveles de la Guerra, los Niveles de Conducción, recursos y finalidad

Fuente– ROB 00-01 Conducción para las Fuerzas Terrestres

Por lo tanto, buscando entender la estrategia argentina, verificase que a nivel de estrategia nacional, las acciones se concentran con a ONTI bajo de la responsabilidad del Gabinete de Ministros del Poder Executivo y se encarga de establecer las políticas del sector y los objetivos políticos que serán alcanzados. Este nivel es fundamental a

integración con las infraestructuras civiles esenciales del país. Así, el nivel estratégico militar, están el Comando Conjunto de Ciberdefensa del EMCFFAA, como órgano central irradiador para las FFAA. Este nivel es posible encontrar el Centro de Ciberdefensa del Ejército Argentino que trabaja en lineamento y vinculación técnica con sus órganos subordinados del MD. Tratase de conducir los planeamientos a largo y mediano plazos, y también de empleo a corto plazo del Instrumento Militar, en un ambiente operacional complejo con interacciones entre el ciberespacio y las demás dimensiones del combate de tierra, mar e aire.

El nivel operacional es aquel que enlaza los niveles estratégico militar y el empleo táctico, con la finalidad de alcanzar el Estado Final Deseado Operacional. Sin embargo, hasta la presente fecha no existe una doctrina argentina consolidada sobre el tema. Las particularidades de la ciberdefensa tornan el asunto complejo y con varias posibilidades para ser estudiadas por las FFAA futuramente. Como ejemplo, sería posible dentro del ciberespacio una estructura estratégica cibernética para apoyar una operación táctica de fuerzas convencionales? Considerando que los ciberataques no respectan fronteras, a respuesta es favorable. Pero, la doctrina clásica argentina no habla sobre acciones que no sean de naturaleza táctica.

En la doctrina existen acciones tácticas que podrán ocasionar efectos estratégicos. Como caso de una acción cinética de un misil balístico de largo alcance en una estación de energía enemiga. Pero, al contrario no lo es posible. No existen acciones estratégicas con efectos tácticos. Hoy en día, no hay estructuras de combate cibernéticas en nivel operacional y táctico.

Muchas de las dudas arriba carecen de un mayor profundizado. La consolidación de una doctrina carece de tiempo para consolidación, aplicabilidad y accesibilidad en el escenario actual.

Segundo el Reglamento ROB 00-01 (2014, Cap VIII, p. 53), la Defesa Cibernética dentro de las Operaciones Militares es clasificada como una Operación Complementaria, o sea, con la finalidad de contribuir con una Operación Básica, con acciones involucradas dentro del ciberespacio. Pode aun ser dividida en dos modalidades, directa o indirecta. A primera, cuando tiene la finalidad de vigiar y controlar redes y sistemas aislado o en conjunto. La última, cunado tiene la finalidad de disputar el control del ciberespacio necesario para accionar las fuerzas militares.

La analice del caso histórico de la invasión militar Rusa en la Georgia en 2008, se observó que los ataques cibernéticas llevados a cabo por gobierno ruso a las infraestructuras críticas georgianas ocurrieran simultáneamente y en mismo tiempo de las operaciones de combate básicas ofensivas realizadas por tierra, mar y aire del gobierno ruso.

Varios países del mundo se quedan hoy estudiando la implementación de su doctrina cibernética. El caso brasileiro, a ser apreciado en el capítulo II, vale de motivación para estudio y fuente de inspiración para el caso argentino.

Plan Estratégico para Ciberdefensa

El Plan Estratégico para Ciberdefensa argentino pasa por la adopción de una Metodología de Planeamiento Basada en Capacidades (PBC). Este contexto, la principal medida es contribuir con los medios civiles en desarrollo para una base estratégica de recursos humanos y materiales que pueden ser empleados en provecto de la Defesa Nacional. La visión interdisciplinar del conocimiento cibernético facilita o empleo de tecnologías de forma dual, o sea, de utilidad pública o militar.

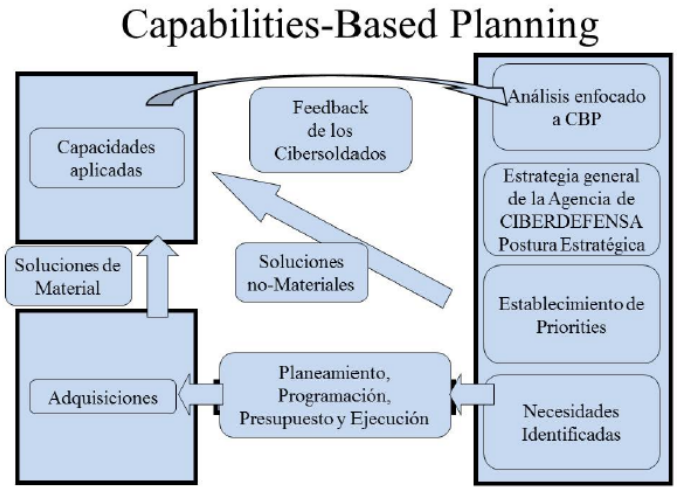
Como citado por Uzal (2013) planear en un ambiente de indeterminación e incertidumbre tiene se transformado en la base de todas las organizaciones. El

Planeamiento Estratégico Informático y de Seguridad de la Informática son ejemplos de planeamientos en unos escenarios cambiantes, turbulentos o imprevisibles. Confundir planeamiento con pronóstico constituye un despropósito insalvable.

Principal desafío es adquirir, desenvolver, fortalecer y ampliar las capacidades que pueden ser empleadas en amplio espectro de amenazas. El punto clave de esta metodología está en canalizar esfuerzos. Ser capaz de proporcionar la viabilidad económica en conformidad con las prioridades apuntadas.

Por lo tanto, el PBC es un planeamiento flexible que se adecue perfectamente al planeamiento para ciberdefensa, lo que permitirá planos más estratégicos y también flexibles. Tendrá al gestor del plan acompañar la evolución de los activos en desarrollos y los mecanismos necesarios para su rápida movilización. Abajo, sigue un dibujo con los constantes *feedback* necesarios para el PBC.

Figura 4 – Visión simplificada del PBC



Fuente – 7º Simposio Argentino de Informática de Estado

Una vez mapeada las necesidades y establecidas las prioridades es posible elaborar el plan propiamente dicho: visión, misión, políticas, objetivos y metas. Así, es posible establecer un programa de trabajo con las tareas correspondientes. Así, para cada amenaza conocida, debe ser establecida una "Línea Base" para su evaluación, donde es

posible identificar cuáles son las vulnerabilidades identificadas y cuales las capacidades que necesitan ser desarrolladas para esas vulnerabilidades.

Conclusiones Parciales

La Defensa Cibernética o ciberdefensa, aún es un concepto bastante nuevo para a consolidación de una doctrina de empleo. Diversos son los conceptos relacionados al tema, con diferentes ópticas y aplicaciones múltiples. Como base en el escenario de conflicto actual del siglo XXI, la mayor parte de los ejércitos del Mundo están buscando entender el fenómeno cibernético y su aplicación militar.

En la Argentina esta realidad no es diferente. Los trabajos académicos sobre el tema aumentaron en la última década y el interés sobre el asunto ya hace parte de estudios en medio civil e militar.

Con relación la Estrategia de Defensa Nacional, el Estado Argentino ya tiene marcos legales regulatorios y estructuras dedicadas al asunto en más alto nivel, como o ONTI, el Comando Conjunto de Ciberdefensa del EMCFFAA, y el Centro de Defesa Cibernética del EA. Registrase que la estrategia de implantación del modelo de más alto nivel para abajo. Todavía, la implantación de un "sistema cibernético" dedicado aún no tiene una solución completa para todos los niveles.

Por fin, cualquier solución futura pasará por una Metodología de PBC. Esa solución dual, integrando esfuerzos civiles y militares, se adecua al desarrollo de un modelo cibernético y contribuirá, futuramente, para el Sector.

CAPITULO II

La estrategia de Brasil para Defensa Cibernética

Finalidad del Capítulo

La Era del Conocimiento, actualmente en marcha, la combinación de las telecomunicaciones con la informática aumentó substancialmente la velocidad con que la información es producida, disponible y almacenada. Segundo la mayoría de las publicaciones especializadas brasileiras, el ciberespacio es un ambiente particular que camina la información. De esa forma, por la doctrina del Ejército Brasileño (EB) la Guerra Cibernética es considerada una capacidad relacionada la Información, siendo un instrumento de empleo militar y una capacidad fundamental para manejo de la Guerra de la Información.

En Argentina, los conceptos de la Guerra Cibernética y la Defensa Cibernética está ampliamente explorados. Sin embargo, en Brasil, además de éstos, el concepto de la ciberguerra está presente en la agenda de los expertos en cuanto a las acciones de carácter ofensivo, como un arma disuasoria real, similar a un dispositivo nuclear. Su origen proviene de 2008, a través del Foro Económico Mundial de Davos. Este fue un año después de la acción masiva de una denegación de servicio ataque cibernético realizado por Rusia contra sitios web del gobierno, bancos y sistemas de energía eléctrica de Estonia. Antes de este facto los ataques cibernéticos que se llevaban a cabo eran esporádicos y aislados. Esta acción masiva se repitió en 2008, cuando la infraestructura de Internet de Georgia se ha caído durante el conflicto con los rusos. En ambos casos, el Gobierno de Moscú se pronunció que los ataques fueron llevados a cabo por grupos de individuos no autorizados. (MANDARINO, 2010, p. 74 e 78).

Las definiciones de ciberguerra varían en función de las obras estudiadas. Según Ferrari (2011, p. 103), el concepto varía de acuerdo con su propósito. Así, ciberguerra es

un conjunto de actos de un Estado contra la soberanía política, económica o de información de otro Estado; en cuanto ciberterrorismo es un ataque cibernético terrorista contra los sistemas informáticos, posiblemente contra la infraestructura crítica en virtud de razones ideológicas o políticas; ya el ciberactivismo (o hacktivismo) es como acciones cibernéticas ideales de activistas con fundamento religioso, político o simplemente para divertirse. Sin embargo, la definición adoptada en el marco de la Defensa Nacional es la que se presenta en el Glosario de las Fuerzas Armadas, MD35-G-01, donde se define como un conjunto de acciones para el uso ofensivo y defensivo de la información y sistemas de comunicación para negar, explotar, corromper o destruir los valores, sistemas de información y redes informáticas, tanto militares cuanto civiles.

Por lo tanto, vale la pena señalar que el trabajo ofensivo o defensivo que la Guerra Cibernética se puede llevar a cabo en las Guerras Regulares o Irregulares, Simétricas o Asimétricas, o mismo de forma aislada.

Aunque la información tramitar dentro del ciberespacio, es posible y deseable que sus efectos tienen lugar en el mundo físico. Tales como el cierre de un corte de suministro eléctrico de central nuclear causando en un hecho en un lugar o tomar un riesgo a la población por radiactividad.

En la literatura de muchos civiles autores, hacen una clara diferenciación entre ataques cibernéticos y la ciberguerra. La primera es el resultado de acciones aisladas sin una conexión con los objetivos estratégicos y operacionales. Tales acciones no son suficientes para considerar esto como una guerra. La ciberguerra requiere el uso coordinado de la fuerza y la intimidación. Para Reglamento del Ministerio de Defensa de Brasil, Doctrina para Operaciones Conjuntas, MD - 30 M-01 (Ministerio de la Defensa de Brasil, 2011), la guerra cibernética incluyen tres tipos de acciones: la exploración; ataque y protección cibernética.

En cuanto a los blancos de la Guerra Cibernética son considerados como un individuo, una sociedad (empresa, institución pública, entidad política, o Fuerzas Armadas) o de un Estado, a condición de que la acción trae una gran ventaja para el atacante. Esto significa que un ataque virtual se seleccionan los objetivos potenciales, que pueden ser designados a nivel objetivos operacional, e incluso un Centro de Gravedad del adversario. Por lo tanto, la infraestructura crítica de un Estado se convertirán en objetivos para los guerrilleros virtuales, y se tornarán parte de la planificación militar de las FFAA.

Antecedentes y marcos legales brasileños

Antes de definir el marco legales brasileño es necesario entender su entendimiento doctrinal de la Seguridad y la Defensa Cibernética y cómo y dónde se debe emplear cada uno.

Según Mandarino (2010, p. 46), ciberseguridad significa proporcionar protección contra el acceso no autorizado, la manipulación y destrucción no autorizada de recursos críticos y activos. Tiene como objetivo mantener la integridad de la infraestructura crítica, principalmente en los sectores de las finanzas, la salud, la energía, el transporte, las telecomunicaciones y la defensa. Puede abordar medidas preventivas y represivas. Las medidas preventivas están relacionados con el establecimiento y la aplicación de metodologías de gestión de riesgos y el desarrollo de planes de contingencia y continuidad de los sistemas sensibles clave. Las medidas represivas incluyen procedimientos para identificar y combatir las actitudes de los cibercriminales. Por último, es posible sintetizar que la ciberseguridad es la prevención y/o represión de las amenazas o fallas en los sistemas informáticos, en especial la infraestructura crítica del país.

En cuanto a la Ciberdefensa comprende acciones operativas, de característica defensivos y ofensivos, pudendo tener inclusive ataques cibernéticos. Por lo tanto, el

Estado debe establecer sus directrices de Defensa Cibernética encaminadas a la restauración inmediata de Ciberseguridad, obviamente, en consonancia con su política de relaciones exteriores.

El Reglamento de Operaciones Conjuntas, MD30-M-01, (Ministerio de la Defensa de Brasil, 2011, p.53) establece la visión del MD con respecto a la Seguridad Cibernética, que se define como "el arte de asegurar la existencia y la continuidad de la Información de una nación, garantizar y proteger en el ciberespacio, sus activos de información y su infraestructura crítica".

Complementa aunque la Defensa Cibernética es un conjunto de acciones defensivas, exploratorios y ofensivas en el contexto de una planificación militar, llevada a cabo en el ciberespacio, con el fin de proteger nuestros sistemas de información para obtener datos para la producción de conocimiento y la inteligencia provocar daños en los sistemas de información del oponente.

El primer marco jurídico brasileño en relación con la cibernética fue la Ley Federal Nº 7.232, que hablaba sobre la Política Nacional de Informática, antes mismo de la popularización de la Internet, que se produjo a partir de los años noventa (Poder Legislativo de Brasil, 1984).

Acerca de los marcos legales brasileños, la clasificación más alta es la Constitución Federal. En el art. 21, III, es el Gobierno Federal que garantiza la Defensa Nacional. Dejando sin duda que la responsabilidad es de todo el Estado, aunque está presente en mismo documento el art. 142, que habla de la competencia de las Fuerzas Armadas para Defensa de la Patria.

Pero el siguiente paso dado en cibernética ocurrió sólo en el año 2000, a través de la Política de Seguridad de la Información, llevado a cabo por la Secretaría de Asuntos Estratégicos y editado por el Decreto Nº 3505 (Poder Ejecutivo de Brasil, 2000).

En 2001, tras los atentados del 11 de Septiembre en los EEUU, se produjo el proyecto y la activación del Gabinete de Seguridad Institucional de Brasil (GSI/PR), la Ley Federal Nº 10638, establece su competencia en las áreas de inteligencia federal y seguridad de la información. En este momento, el tema de la seguridad de la información ganó más importancia en todo mundo, y con ella también la Ciberseguridad (Poder Legislativo de Brasil, 2003).

La Política Nacional de Defensa (2005) ha reforzado los objetivos nacionales establecidos en la Constitución y se pretende involucrar todos los ciudadanos brasileños en la bandera de la Defensa Nacional.

En 2006, el Decreto 5772, creó bajo de GSI/PR, el Departamento de Seguridad de Información y Comunicación (DSIC) con asignaciones operar y mantener el centro de tratamiento y respuesta a incidentes para tratamiento y control de las redes informáticas de la Administración Federal, llamada CTIR.gov (Poder Ejecutivo de Brasil, 2006).

En 2008, el presidente Lula aprobó la Estrategia Nacional de Defensa (END), y determinó tres principales Direcciones básicas para el desarrollo de la Defensa Nacional, el sector de la energía nuclear, el sector espacial y el sector cibernético. Este documento sirvió de orientación básica del Ministerio de Defensa para conducta de cada uno de estos vectores, considerando la naturaleza y las capacidades establecidas en cada Fuerza. La Armada se quedó con la gestión de las acciones vinculadas al sector nuclear, principalmente debido al actual avanzado y desarrollo del primer submarino nuclear brasileño de propulsión nuclear. La Fuerza Aérea comenzó a concentrar esfuerzos en la continuidad en su desafío de lograr éxito en el Vehículo de Lanzamiento Satélite (VLS). Por último, el Ejército brasileño pasó a liderar las acciones del sector cibernético.

Así, en 2009, el Comandante del Ejército instituyó a través de la Portaria Nº 03 de 29 de junio de 2009, el sector cibernético en el Ejército Brasileño (EB), la formulando

directrices que incluyen, acciones desde la capacitación de recursos humanos hasta la creación de un Núcleo de Centro de Defensa Cibernética.

Ese mismo año, 2009, el DSIC/GSIPR, amplía las acciones en el área de Seguridad Cibernética en toda la Administración Federal, con la creación de Equipos de Tratamiento y Respuesta a Incidentes en Redes de Computadores - ETIR.

Dentro del Ministerio de Defensa, el desarrollo de la Defensa Cibernética se ha convertido en una necesidad prioritaria para las tres Fuerzas funcionaren sincronizadas y en red. A nivel operativo, está la importancia de las operaciones conjuntas coordinadas por el Estado Mayor Conjunto de las Fuerzas Armadas (EMCFA).

El Libro Verde de Seguridad Cibernética brasileña, dirigido por la DSIC del GSI/PR, reglamento básico para la formulación del Libro Blanco de Defensa Nacional, presenta la Política Seguridad Cibernética dividida en varios vectores: político-estratégico, económico, social y ambiental, científico y tecnológico, educación, cooperación internacional, y seguridad de infraestructura críticas (MANDARINO y CANONGIA 2010, p. 24 y 49).

En 2010, el EB ha dado el paso más largo en la consolidación de su joven carrera del Sector Cibernético. Por medio de la Portaria N ° 666 y N ° 667 del Comandante del Ejército se activó el Centro Cibernético de Defensa del Ejército (CDCiber) que tiene sus propias instalaciones, personal especializado y material.

Figura 5 – Centro de Defesa Cibernética

Fuente - Revista Operacional Brasil [11]

[11] Revista Nacional. Recuperado: http://www.revistaoperacional.com.br/2015/exercito/exercito-brasileiro-

Desde la creación de CDCiber el EB ha estado entrenando sus recursos humanos para el sector en el Centro de Enseñanza de Guerra Electrónica (CIGE), dividido a gran afinidad entre las actividades de Guerra Electrónica y Cibernética. Los cursos de Guerra Cibernética promovidas por CIGE son responsables por la formación y especialización de los expertos para el CDCiber y otras Militares Organizaciones relacionadas del Sector, allá de contribuir con las otras Fuerzas Armadas y otros órganos de la administración pública.

El CDCiber tuvo muy buena participación en los principales eventos que Brasil fue anfitrión en los últimos años, como la Conferencia Río + 20, los Juegos Mundiales Militares, Jornada Mundial de la Juventud, la Copa de las Confederaciones de Fútbol y la Copa del Mundo de Fútbol. Este resultado validó la estructura del CDCiber y proyectó el próximo paso para la creación de la Escuela Nacional de Defensa Cibernética, actualmente en fase de diseño, con el esfuerzo conjunto de científicos de la Universidad de Brasilia. La intención es crear una estructura para certificación y análisis de amenazas forense.

Después de que el virus "Stuxnet" sorprendió al mundo en 2010, causando principalmente pérdidas para el programa nuclear iraní, los gobiernos y los expertos han intensificado la búsqueda de soluciones nacionales para regular el internet en sus países. Este año China dio a conocer el "*Great Cannon*" (Gran Cañón) con el fin de dirigir el flujo de los internautas extranjeros que ingresen al país para un sitio de control gubernamental. El país asiático asegura que la intención es sólo para uso defensivo y para censura, pero los expertos dicen que puede ser utilizado como una arma cibernética para degradar las infraestructura crítica de otro país.

A pesar de las acciones ofensivas de Guerra Cibernética no son de naturaleza cinética, puede causar grandes trastornos en la población y consecuencias físicas

---

fortalece-mais-a-sua-defesa-cibernetica-no-pais

irreparables. Por lo tanto, en la actualidad, hay una discusión de estas acciones son suficiente para justificar una respuesta armada de un país atacado. Hay tres escuelas de pensamiento, el primero, de acuerdo con Clark (2010, p. 63), respaldase en la tesis de la omisión de la Carta de la ONU, donde se afirma que interrumpir las comunicaciones enemigas que no implica el uso de la Fuerza, lo que lleva a interpretar que los ataques a los sistemas actos informatizados no serán considerados de guerra. La segunda interpretación, según Murphy (2010, p. 24), evalúa los ataques cibernéticos de acuerdo con los efectos causados que pueden ser de gran magnitud, que pueden llevar un perdida a la soberanía del Estado, lo que justificaría la acción armada. Por último, la tercera corriente defendida por Lewis (2010, p. 08), cree que los pequeños actos causados por personas aisladas, a pesar de que están violando la soberanía del Estado, no representan actos de guerra, pero si se emplean estos actos todos los días y en grandes cantidades, puede ser considerado un acto hostil, llevando la legitimidad de acciones de fuerzas.

La Defensa Cibernética en Ejército Brasileño

La doctrina brasileña, tal cual como la argentina, realiza una división didáctica de cuatro niveles de la conducción. Sin embargo, en el más alto nivel de la Estrategia Nacional (Estrategia Gran) se clasifica en Brasil como a Nivel Político, dejando el concepto de "estratégica" dedicado exclusivamente a parte sectorial de la Defensa Nacional, realizada por el Ministerio de Defensa. Los otros niveles bajo, operacional y táctico, son similares en ambos países.

Los conceptos ya presentados a la Seguridad Cibernética y la Defensa Cibernética, el Ministerio de Defensa de Brasil clasifica las acciones en el ciberespacio en tres niveles. El Nivel Político se llama **Seguridad de la Información y Comunicaciones (SIC)**, que se lleva a cabo por el GSI/PR, que abarca un concepto más arriba del ciberespacio. Este

conocido como **Seguridad Cibernética**, corresponde a participación de todos los organismos del Gobierno Federal y de las infraestructuras nacionales de infraestructuras críticos del sector público y privado. El Nivel Estratégico corresponde a la **Defensa Cibernética**, con las acciones llevadas a cabo por el Ministerio de Defensa en coordinación con otros ministerios y el propio GSI/PR. A Nivel Operacional y Táctico las acciones son llamadas de la **Guerra Cibernética**, quedando las acciones dependientes de cada Fuerza Armada (CARNEIRO, 2012, p. 116).

La siguiente ilustración presentada por Carvalho (2011) y modificada por Pasini (2014) muestra la división por niveles de conducción.

Figura 6 - Integración entre Seguridad y Defensa Cibernética

NÍVEL	DENOMINAÇÃO	ÓRGÃO DE COORDENAÇÃO
Político	Segurança da Informação e Comunicações (SIC) Segurança Cibernética	Gabinete de Segurança Institucional da Presidência da República (GSI-PR)
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional	Guerra Cibernética	Forças Armadas – Comando Conjunto
Tático		Forças Armadas – Força Componente

Fuente - CARVALHO (2011, p.43), modificado por PASINI (2012, p.70)

La Doctrina de Seguridad y Defensa Cibernética tiene como objetivo proporcionar la seguridad nacional, con la finalidad de garantizar el país contra amenazas contra las personas, instituciones o benes y servicios existentes en el país. Estos ataques en el ciberespacio interfieren en el entorno físico, pudendo afectar a los asuntos internos y la política estatal.

Según Mandarino (2009), la Guerra Cibernética consiste en atacar informaciones dentro del ciberespacio, haciendo uso de diversas formas de acción, del terrorismo hasta la destruición de infraestructura total de la información, causando asimetría de poder económico, capacidad militar, y estructuración organizativa de una Nación. Estas acciones

visión obtener ventajas civiles o militares.

Por lo tanto, la modernización de los sistemas militares trae vulnerabilidades que permiten acciones que pueden interrumpir las redes de computadoras a sistemas de armas. Afecta a los que necesitan de sincronización de acciones en tiempo y espacio, afectando el liderazgo y capacidad de toma decisiones en diferentes niveles.

Así, una doctrina cibernética alineado en todos los niveles es necesario, involucrando a los diversos actores que se dedican a la Seguridad de Informaciones y Comunicaciones en el Gobierno Federal, con el objetivo de actuar como un Estado Nación, con el fin de facilitar y asegurar su disponibilidad, integridad, confidencialidad y autenticidad.

La Doctrina Militar de Defensa Cibernética (2014), reglamento del Ministerio de Defensa, organiza los niveles de responsabilidad y organiza la forma de empleo del Sector Cibernético. Nivel Político la Presidencia de la República, a través del GSI/PR e del Comité Gestor de Internet en Brasil encaminan las directrices generales. La aplicación práctica de las acciones correrán a cargo CTIR.Gov en coordinación con el CERT.br. Son estructuras desplegadas en todo país para control, seguridad, y tratamiento de incidentes de red. Sus acciones enlazan todos los organismos de la Administración Federal e infraestructuras críticas y empresas colaboradoras de interés para la Defensa Nacional.

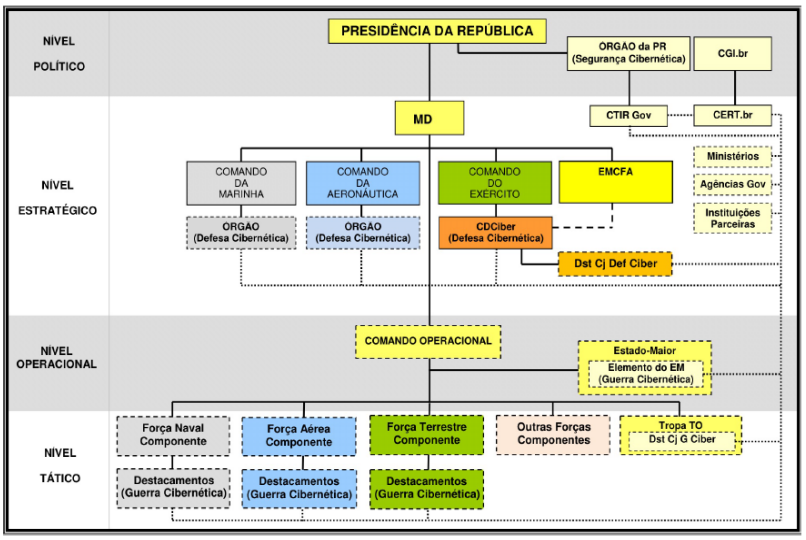
El Nivel Estratégico de Defensa Nacional, el CDCiber del Ejército es el órgano de coordinación de las acciones, involucrando de organismos similares de otras fuerzas armadas. Su objetivo principal es el desarrollo de habilidades y proporcionar las mejores condiciones posibles para la ejecución de acciones en los niveles inferiores. De forma temporaria puede formar un Destacamento Conjunto de Defensa Cibernética (Dst Cj Def Ciber) con la finalidad de conducir acciones estratégicas de Defensa Cibernética, como ocurrido en los grandes eventos, como la Copa del Mundo de fútbol, en 2014.

En Nivel Operacional, la estructura adoptada dependerá de la misión, el enemigo, el

tiempo, ambiente operativo, y los medios puestos a disposición. Normalmente, las acciones se realizan en forma conjunta y centralizada, mediante un Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber).

Abajo se encuentra la estructura y órganos en el diseño del Sistema Militar de Defensa Cibernética según lo establecido por la Doctrina del Ministerio de Defensa

Figura 7 – Estructura y órganos del Sistema Militar de Defensa Cibernética



Fuente - BRASIL, Doutrina Militar de Defensa Cibernética, 2014.

La Seguridad Cibernética en Nivel Político

En Nivel Político la coordinación es del GSI/PR. Las estructuras bajo de su organización son responsables de identificar amenazas tempranas para evitar la expansión de los daños causados. El control de vulnerabilidades es una preocupación constante de los mecanismos de control.

Para que se produzca esta coordinación es necesario conocer las funciones de los principales órganos de la Administración Federal relacionados con la Seguridad Cibernética, así citado por (DRUMOND, 2014. p.19).

Agencia Brasileña de Inteligencia (ABIN) - evaluar las amenazas internas y externas a la orden constitucional, incluyendo la cibernética. Cuenta en su estructura organizativa, con el Centro de Investigación y Desarrollo de Seguridad de Comunicaciones (CEPESC),

que promueve la investigación científica y tecnológica aplicada a la seguridad de las comunicaciones. Su tarea principal es coordinar las acciones inherentes al Sistema Brasileño de Inteligencia (SISBIN) relacionados con el Sector Cibernético.

Agencia Nacional de Telecomunicaciones (ANATEL) - Promover el desarrollo de las telecomunicaciones en el país. Monitoriamente del espectro de radio frecuencia en los rangos para la transmisión de datos de dispositivos móviles identificados como de interés para la Defensa Cibernética.

Cámara de Relaciones Exteriores y Defensa Nacional (CREDEN) - órgano asesoramiento de la Presidencia de la República en los asuntos relacionados con las relaciones exteriores y la Defensa Nacional. Aprobar, promover la articulación y coordinación de medidas establecidas, que van allá de la competencia de un solo Ministerio.

Casa Civil de la Presidencia de República - Es para la asistencia directa de la Presidencia. Tiene las funciones relacionadas con la aplicación de las políticas y normas técnicas y operativas adoptadas por el Comité Gestor de Infraestructuras de Clave Públicas Brasileñas (ICPBrasil).

Comité Gestor de la Internet en Brasil (CGI.br) – Propone normas y procedimientos relativos a la regulación de las actividades de la internet, además establecer directrices estratégicas relacionadas con su uso en Brasil. Colaborar mediante el intercambio de información sobre detección de incidentes, correlación de eventos y determinación de tendencias de ataques en el ciberespacio, con capacidad de comprometer las acciones militares.

Consejo de Defensa Nacional (CDN) - órgano de consulta del Presidente de la República en los asuntos relacionados con la soberanía y la Defensa del Estado

democrático de derecho. Tratar asuntos relacionados con la Seguridad de la Información y de las Comunicaciones, Seguridad Cibernética y Seguridad de infraestructuras críticas.

Departamento da Policía Federal (DPF) por medio de Centros de Defensa Cibernética – Coordinar y ejecutar acciones relacionadas actos ilegales criminales practicados contra la Seguridad de la Información y Comunicaciones. Llevar a cabo intercambio de información a través del canal técnico sobre los crimines detectados en el ciberespacio que pueden influir en la Defensa Nacional.

Departamento de Seguridad de la Información y Comunicaciones (DSIC) – Tiene la atribución operar y regular las actividades de la SIC en el Gobierno, de la capacitación de los funcionarios civiles federales, así como los contratistas, sobre la SIC; la realización de los acuerdos internacionales para el intercambio de información confidencial; representación del país junto a Organización de Estados Americanos (OEA) para los asuntos de terrorismo cibernéticos; y el mantenimiento de los Centro de Tratamiento y la Respuesta de Incidentes de red (CTIR.Gov). Contribuye a la Seguridad Cibernética con las acciones de mantenimiento del Centro Tratamiento de Respuesta a Incidentes.

Servicio Federal de Procesamiento de Datos (SERPRO) - a través de su Grupo de Respuestas a Ataques (GRA) - Realizar la seguridad de los sitios del gobierno bajo su administración. Colabora mediante intercambio de información de detección de incidentes, con la correlación de eventos y determinación de tendencias de ataques en el ciberespacio.

La Defensa Cibernética en Nivel Estratégico

El Nivel Estratégico tiene necesidades fundamentales de coordinación y concentración. Tiene las mismas atribuciones de coordinación del nivel político, además de tener que centralizar los esfuerzos para lograr una mejor interoperabilidad y sinergia de sus medios.

La Defensa Cibernética tiene necesidad de aumentar la coordinación no sólo entre las FFAA, sino también para otros organismos del Estado, a través de los vínculos entre sus sistemas de Comando y Control. Sin embargo, la conducción de las acciones deberá siempre ser llevada a cabo por el Ministerio de Defensa, asesorado por EMCFA, debido a su capacidad de integrar otras capacidades relacionadas con la Defensa Nacional. Así, el Ministerio se convierte en el único vínculo entre los Niveles Política y Operacional.

Distinta de la estrategia argentina, el Ministerio de Defensa de Brasil **no** optó por la creación de un "**Centro Conjunto de Defensa Cibernética**", solamente ampliando las estructuras y capacidades de los ya existentes CDCiber del EB, quedando sólo el EMCFA con los deberes de la coordinación y conducción de las actividades.

En este Nivel, el EMCFA través CDCiber, a través de sus órganos de Defensa Cibernética de las otras FFAA, además de los Centros de Tratamiento de Incidentes de Red (CTIR) de la Administración Pública, así como otras instituciones asociadas, coordina la planificación y ejecución de acciones para mantener actualizadas las amenazas al Brasil en el ciberespacio.

El Destacamento Conjunto de Defensa Cibernética es una estructura formada para llevar a cabo gran parte de las habilidades necesarias para la Defensa Cibernética. En los últimos años, fruto de los grandes eventos que Brasil fue sede, fue una herramienta fundamental para el logro de acciones estratégicas y ofrecer mejores condiciones en los niveles operacional y táctico.

Esta estrategia es el resultado de las principales características y limitaciones causadas por la explotación del ciberespacio. Entre la dificultad principal está en identificar la fuente del ataque cibernético; la casi imposibilidad de mantener la invulnerabilidad de sus propios sistemas informáticos; dificultades para identificar y reclutar talento humano; vulnerabilidad a los ataques de las acciones asimétricas; y, por

último, una gran dificultad en el seguimiento de los avances tecnológicos.

Según el reglamento Operaciones de Información, EB 20 - MC 10 213 (Ejército Brasileño, 2014), son posibilidades de Defensa Cibernética:

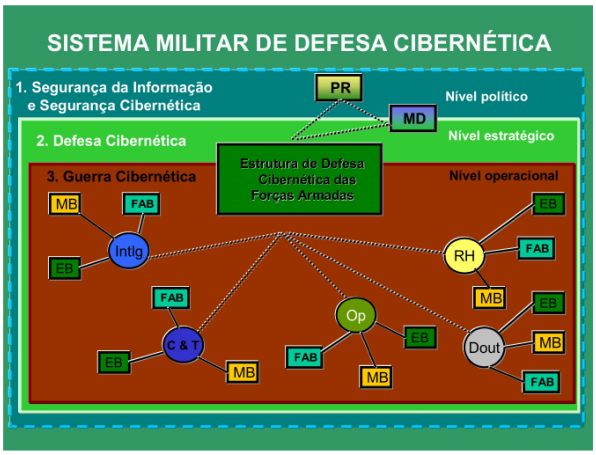
- Actuar en el ciberespacio, a través de acciones ofensivas, defensivas y exploratorias;
- Cooperar con la producción de conocimiento de inteligencia - Fuente Cibernética;
- Lograr la infraestructura crítica de un oponente sin límites de alcance físico y exposición de tropas;
- Cooperar con los organismos externos de Seguridad Cibernética del Ministerio de la Defensa por medio de una solicitación o en el contexto de una operación;
- Cooperar con el esfuerzo de movilización para garantizar la capacidad de disuasión;
- Obtener la sorpresa más fácilmente, basado en la capacidad de explotar las vulnerabilidades de los sistemas de información del oponente;
- Tomar medidas contra oponentes más fuertes, en el concepto de guerra asimétrica; y
- Realizar acciones con costos significativamente más bajos que las operaciones militares en otros dominios.

Para la Doctrina de Defensa Militar (Ministerio de la Defensa de Brasil, 2014), la Defensa Cibernética comprende un conjunto de acciones ofensivas, defensivas y exploratorias, que se celebran en el ciberespacio. Por lo tanto, hay tres tipos de delitos cibernéticos: el **ataque cibernético** dirigido para interrumpir, negar, degradar, corromper o destruir los sistemas de información computacionales; **protección cibernética** que tiene como objetivo neutralizar ataques y explotación cibernéticas de sus propios dispositivos y redes de informática; y la **exploración cibernética** que consiste en acciones de búsqueda o coleta en los Sistemas de Tecnología de la Información de interés para obtener el conocimiento de la situación del medio cibernético.

El Ministerio de Defensa por EMCFA concibe y coordina el Sistema Militar de

Defensa Cibernética (SMDC) que tenía por objeto mejorar la gestión de las capacidades bajo su alcance para garantizar los intereses de la Defensa Nacional. Este sistema también es responsable de proporcionar protección al Sistema Militar de Comando y Control que le permite trabajar en red de forma segura de ejecutar la coordinación e integración de las informaciones de la infraestructura crítica. En la figura siguiente se presenta por Carvalho (2012), verificase la estrategia de concentrar capacidades de las FFAA para desarrollo conjunto de los vectores básicos de defensa cibernética: Inteligencia, Recursos Humanos, Doctrina y Operaciones. Esta concentración que se produjo en el Nivel Estratégico es también común en Nivel Operacional.

Figura 8 - Sistema Militar de Defesa Cibernética



Fuente - CARLAHO, 2012 citado por DRUMOND, 2015

El CDCiber es el órgano central de SMDC y pasa el Comando de Operaciones del Ministerio de Defensa para Operaciones Conjuntas, contando de forma permanente de un Estado Mayor Conjunto para planificación y control de acciones.

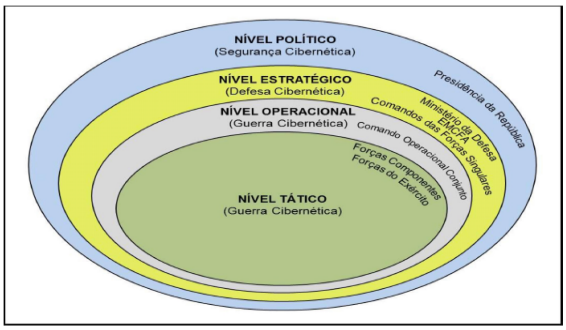
Entre los deberes de CDCiber está en mantener la doctrina militar actualizada del sector cibernético; fomentar el desarrollo y el intercambio de tesis y otros trabajos similares, con el enfoque doctrinario en las instituciones de educación superior de carácter civil y militar de interés al sector cibernético; inserte la Defensa Cibernética en ejercicios de simulación y de combate y las operaciones conjuntas; crear un sistema gestión de

conocimiento de lecciones aprendido para actualizar permanentemente la doctrina; y, finalmente, proponer actualizaciones de doctrina para el sector cibernético.

La Guerra Cibernética en Nivel Operacional y Táctico

Para la doctrina de Operaciones de Informaciones brasileña, la Guerra Cibernética es empleada en los niveles operacional y táctico y corresponde al uso ofensivo y defensivo de informaciones y sistemas de informaciones para negar, explorar corromper, degradar o destruir capacidades de comando y control enemigas (Ejército Brasileño, 2014, p.4-8).

Figura 9 - Níveles de decisión de Operaciones Cibernéticas



Fuente - Operaciones de Información – EB 20-MC 10.213

En Nivel Operacional son realizados todos los planes militares para la Campaña, como base en los planes existentes formulados por las Hipótesis de Empleo y por las directrices recibidas de los niveles superiores. Las fracciones militares de empleo son conformadas segundo sus características y capacidades. El mismo pasa en la Guerra Cibernética donde necesita un alto grado de especialización.

La formación temporaria de una Célula de Operaciones e Información es una estructura que normalmente es empleada para las Operaciones Militares Conjuntas conducidas en Nivel Operacional. Para tener el control de la información, esta célula consta con especialistas de las principales capacidades relacionadas a la información. Los militares de Guerra Cibernética trabajan en sinergia de esfuerzos con otros militares para el

logro de resultados útiles para el Comandante Operacional.

Allá de esta estructura arriba, formase un Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber) que reunirá especialistas de diversas áreas, civiles o militares, inclusive de otras Fuerzas, para trabajar técnicamente para alcanzar objetivos definidos por el Comandante Operacional y factibles de ser alcanzados por el Destacamento. Esta estructura tiene un enlace técnico con el Dst Cj Def Ciber, conducido por CDCiber, con finalidad de contribuir el logro de sus resultados.

Segundo la Doctrina Militar de Defesa Cibernética (Ministerio de la Defensa de Brasil, 2014) las actividades del Dst Cj G Ciber tiene las siguientes posibilidades:

- identificar y analizar vulnerabilidades (conocidas) en las redes de computadores y aplicaciones empleadas en Sistema de comando y control desplegado para la operación;

- recomendar acciones para mitigar las vulnerabilidades identificadas;

- estudiar las amenazas y entender su impacto en las redes de C2 o cualesquier otras estructuras/recursos computaciones de las fuerzas amigas;

- verificar la conformidad de Seguridad de la Información y Comunicaciones en el Sistema de Comando y Control desplegado para la operación;

- planear y ejecutar acciones cibernéticas (protección, exploración y ataque), en el contexto de la operación conjunta, con apoyo de los órganos de Defesa Cibernética de las FFAA en cumplir a las orientaciones y directrices emanadas del Comando Operacional;

- asesorar los Comandantes de todas las Fuerzas Singulares en las solicitaciones de efectos deseados;

- colaborar con las acciones planeadas por la Célula de Op Info; y

- colaborar con los esfuerzos de obtención de datos para la producción de conocimiento de Inteligencia, por intermedio de la Fuente Cibernética, en contexto de la operación conjunta.

Segundo Drumond (2014, p.42), el Dst Cj G Ciber ya está siendo ampliamente empleada en Operaciones Militares de responsabilidad del Ministerio de la Defensa y conducidas por las FFAA. Así, este autor presenta ejemplos de Operaciones donde fueron empleados con logro esta conformación.

- Operación Anhanduí (año de 2011);
- Operación Amazonia (año de 2012);
- Operación Atlántico III (año de 2012);
- Río + 20 (año de 2012);
- Operación da Jornada Mundial da Juventud (año de 2013);
- Operación Ágata (año de 2013);
- Operación Lazador (año de 2013);
- Copa de las Confederaciones de Fútbol (año de 2013); e
- Copa del Mundo de Fútbol (2014), entre otras Operaciones.

En Nivel Táctico, la Organización Militar responsable en recursos para conformar Destacamento de Guerra Cibernética de la Fuerza Terrestre es el 1º Batallón de Guerra Electrónica (1º BGE).

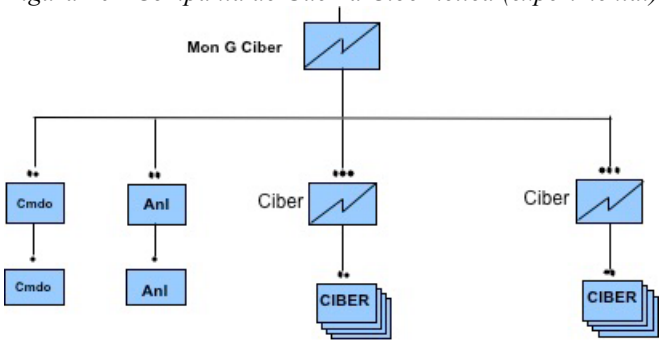
La estructura experimental del 1º BGE tiene por finalidad capacitar la Fuerza Terrestre con medios de Guerra Electrónica y Guerra Cibernética. Esta nueva estructura sigue la tendencia tecnológica de aproximación (o mismo fusión) de tráfico de informaciones circulante en espectro electromagnético y en ciberespacio. Hoy en día, la mayor parte de los equipos radios de comunicaciones militares son digitales, controlados o definidos por *softwares*, como los actuales *smartphones* de empleo civil.

Para eso, el 1º BGE fue estructurado con una Compañía de Guerra Electrónica (Cia GE) y otra de Monitoreo y Guerra Cibernética (Cia Mon Ciber), además una tercera Compañía de Apoyo. Esa estructura tripartida, permite conformar distintos módulos con

capacidades diferentes para impedir, explorar, degradar, atacar o tirar es una ventaja de los sistemas informatizados de campaña y redes radio enemigas.

La Cia Mon Ciber fue conformada para tener características de gran flexibilidad, con la finalidad de atender una demanda de ocho destacamentos.

Figura 10 - Compañía de Guerra Cibernética (experimental)



Fuente - DRUMOND, 2014

Las principales acciones tácticas para empleo de la Guerra Cibernética son citadas por Ferrari (2011, p.94), conforme expuso a seguir. Muchas de esas acciones presentan bajo costo de investimento y pueden ser realizadas de cualquier lugar con acceso a la internet. El objetivo principal explorar fallas de seguridad en sistemas informatizados y/o de *softwares* de seguridad, antes que el usuario descubra. Eses ataques tienen por finalidad incapacitar totalmente blancos o afectar sus funcionalidades, repercutiendo en la disponibilidad, confidencialidad, autenticidad e integridad de los servicios.

Adquisición de información - por medio de "Caballos de Troya" u otros *softwares* y virus destinados a obtener datos y/o informaciones del oponente para empleo contra él mismo o terceros;

Alteración, corrupción, sabotaje o descaracterización de la información - este último también conocida como *defacement* (descaracterización de una página en la internet). La alteración y corrupción de la información pueden ser realizadas de muchas formas, pero principalmente por el método llamado en algunas bibliografías de "ataque del hombre del ambiente", que consiste en la información ser alterada (en medio del camino) por alguien

antes que ella llegue al su destino final;

Injección de *Structured Query Language* (SQL) - para robar informaciones, como claves y datos financieros o para dar al hacker el control general no autorizado de servicios (engañando sistemas de seguridad) permitiendo el control de sistemas, principalmente los de infraestructuras críticas, a distancia;

Ataque distribuido de negación de servicios (*Denial of Service* - DoS) - para degradar los medios de computaciones. Ese ataque consiste en comandar, por la red, varios computadores de usuarios conectados a internet, sin que este perciba, para acezar simultáneamente una determinada página en la internet, sobrecargando el servidor de la institución/empresa doña del *site*, e así, haciendo con que ele pare de funcionar por algunas horas o días.

Destruición física de determinado componente - de un equipo/sistema informatizado, o de toda su estructura, por medio da inserción de virus. Un ejemplo fue el caso ocurrido con la difusión del "Stuxnet", que fue criado para sabotear fábricas y perjudicar sistemas industrias, principalmente de las usinas nucleares de Iran, en 2009. Segundo Berman (2011, p. 45) la antigua coordinadora nacional de Seguridad Cibernética del os EEUU, Melissa Hathaway, opinó en la época, que el "Stuxnet" representaba un tipo cualitativamente nuevo de Guerra Cibernética y que ninguno país está preparado para lidiar con él. La diseminación del virus puede ser de varias formas, como por la internet, por un hacker a distancia o por envío de virus por alguno artefacto o *pen-drive* de un aliado, espía o un funcionario desavisado; y

Ingeniería social- donde los hackers exploran la curiosidad, la ganancia o miedo del usuarios, con mensajes del tipo "su mujer está te traicionado, click aquí, crédito fácil, etc". Después de convencer el usuario a meterse en link falso, el hacker tiene libre acceso a su computadora, a veces sin que el usuario perciba que está contaminado. Así, él podrá robar

datos financieros, usar su cuenta de e-mail y hacer espionajes industriales, allá de que el computador podrá quedar, por meses, bajo el mando del hacker y así ser usado para atacar otras víctimas por medio del internet, o por la diseminación con aquivos de *pen-drive*.

Conclusiones Parciales

En Brasil la Seguridad Cibernética tiene una clara división entre los cuatro niveles de la conducción, el que confirma una preocupación estatal para el tema. En Nivel Político, el sector es llamado de Seguridad Cibernética, bajo responsabilidad del GSI/PR; el Nivel Estratégico, sectorial para Ministerio de la Defensa, corresponde a Defensa Cibernética; e Niveles Operacional e Táctico tiene la responsabilidad de conducir las acciones relativas a Guerra Cibernética, bajo la responsabilidad de las FFAA.

La Estrategia Nacional de Defesa (END), de 2008, fue un marco para el Sector Cibernético Nacional. Elevó el tema al más alto nivel de prioridad del Estado Brasileño, juntamente con los sectores nuclear y espacial. Determinó aunque el EB seria la Fuerza inductora para el desarrollo y empleo del tema.

Los grandes eventos que Brasil tiene hospedado, sirven para desarrollar y consolidar la doctrina de empleo del sector. Posibilita aun el acúmulo e entrenamiento para nuevas estructuras criadas por EB, como el CDCiber y el 1º BGE.

Conclusiones Finales

Las primeras manifestaciones de que el escenario del campo de batalla estaría cambiando acorrieron en los fines del siglo XX con lo concepto de Era del la Información, después, más recientemente, llamada de Era del Conocimiento. La información pasó a ser explotada como una herramienta fundamental para la ampliación del poder de combate. El desarrollo tecnológico impulsó que las informaciones pasasen a ser masivas y, a veces en tiempo real, decidiendo los combates modernos, donde el tiempo es factor fundamental para la toma de decisiones.

Los medios que esta información se puso en marcha dejaron de ser físicos y pasaron a dominar el espectro electromagnético. Poco más tarde, las comunicaciones radio pasaron a ser digitales, de gran capacidad de transmisión, como los actuales *smartphones* que hacen parte de las vidas de todas las personas. En este mismo tiempo, las comunicaciones virtuales también se ampliaron, con la popularización de la internet. El uso de PCs y notebooks se tornaron fundamentales para utilización en los días de hoy, sea en complejos sistemas corporativos o para diversión diaria en las residencias.

Con este escenario, dominar el ciberespacio pasó a ser fundamental para la gerencia de los riesgos y amenazas contra la Defensa Nacional. Por lo tanto, Argentina y Brasil tienen estrategias parecidas para desarrollar y emplear capacidades del sector cibernético, con pequeños puntos de distinción.

A partir del año 2008 y 2009, con los ataques cibernéticos realizados en Estonia y Georgia, supuestamente realizado por Rusia, despertaron la preocupación de todo mundo para los riesgos de ataques cibernéticos coordenados con operaciones militares convencionales. En estos ejemplos, en apoyo cibernético pasó como una Operación Complementar. Todavía, en 2010, con el ataque de virus “Stuxnet” a las instalaciones de desarrollo del programa nuclear iraní, las operaciones cibernética pasaron a ser también

desplegadas como operaciones de origen estratégicas, pero sin una identificación clara del agresor. En la Sudamérica, Argentina y Brasil siguen la tendencia mundial y empezaron sus respectivos desarrollos del Sector Cibernético.

Argentina firmó sus primeros marcos legales específicos para el Sector Cibernético fue la edición de la Resolución Nº 580/2011 (Poder Executivo Nacional, 2011) que creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) bajo de la Oficina Nacional de Tecnologías de Información (ONTI).

Siguiendo las iniciativas civiles, las FFAA empezaron los trabajos conjuntamente con la Resolución Nº 343/MD, de 14 de mayo de 2014 que creó el Comando de Conjunto de Ciberdefensa bajo el EMCFFAA. El EA sigue la estructura de arriba y también conforma su estructura propia, en 14 de noviembre, el Centro Cibernético del Ejército bajo al Jefe de Estado Mayor General del Ejército.

Actualmente, el Estado argentino y sus FFAA concentran esfuerzos en acciones de arriba para abajo, en proseguimiento del Plan Estratégico para Ciberdefensa, buscando identificar y desarrollar las capacidades esenciales.

En Brasil se busco primer una identificación de los principales conceptos, como Seguridad, Defensa y Guerra Cibernética. Estas distinciones son fundamentales para la organización de los niveles de la conducción. La Seguridad Cibernética es una responsabilidad de todo el Estado Brasileño, conducido por el Nivel Político (o Estratégico Nacional, en la Argentina), por el GSI/PR. La Defensa Cibernética es una responsabilidad de la defensa Nacional y conducida por el Ministerio de la Defensa. La Guerra Cibernética, además de las acciones defensivas es posible encontrar actitudes ofensivas, y deberá ser conducida por los niveles operacional y táctico.

Para poner en marcha la organización arriba, fue fundamental la edición de la Estrategia Nacional de Defensa (END), en 2008. Concentró las actividades bajo la

coordinación del EB que creó el Centro de Defensa Cibernético (CDCiber). Este estructura pasó a ter enlaces con varios órganos de interés para el Sector Cibernético nacional, como el Departamento de Seguridad de Información y Comunicación (DSIC) del GSI/PR, que ya tenia sido creado en 2006.

Para empleo de acciones estratégicas, el CDCiber coordina y conforma acciones a través del Destacamentos Conjunto de Defensa Cibernética, principalmente para acompañamiento de operaciones de gran magnitud, como las que Brasil tiene hecho en los últimos años. Para los niveles operacional y táctico, la estructura es el Destacamentos Conjunto de Guerra Cibernética que labura en sintonía con el Destacamento equivalente de arriba y bajo el mando del Comandante Operacional.

Por fin, Argentina y Brasil están lejos de llegar a una posición consagrada, principalmente por la dinamismo del tema. Pero ambos presentan la opción acertada de mirar la mejor forma de combatir la guerra del futuro.

Referencias

ARGENTINA. *Sitio Oficial*. Oficina Nacional de Tecnologías de la Información. http://www.icic.gob.ar/

BERMAN, Ilan. (2011). *Iranian Cyberwar, U. S. Must Prepare for Possible Confrontation*. Defense News.

CANDELA, Justribó; SOL, Gastaldi; FERNANDÉZ, Jorge A. Escuela de Defensa Nacional (EDENA). *Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político - institucional y normativo*. Recuperado de: http://www.edena.mindef.gob.ar/docs/PERFIL_DOCUMENTOS/GASTALDI_1.pdf

CARNEIRO, J. M. (2012). *A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro*. Tesis (Doctorado en Ciencias Militares) – Escola de Comando e Estado-Maior. Rio de Janeiro/Brasil

CARVALHO, Paulo Sérgio M. (2011). *A Defesa Cibernética e as Infraestruturas Críticas Nacionais*. In: X CICLO DE ESTUDOS ESTRATÉGICOS: PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS. Escola de Comando e Estado-Maior. Rio de Janeiro/ Brasil. p. 38-53.

CLARK, Blane R. (2010). *As Operações de Informações como um Elemento Dissuasório do Conflito Armado*. Militar Review. Ed. Brasileira.

Diario Clarín. Recuperado de: http://www.ieco.clarin.com/tecnologia/estadisticas-Internet-millonesenviados-minuto_0_1167483520.html., 25 de julio de 2014.

DRUMOND, J. M. (2014). *A Guerra Cibernética no Nível Operacional / Tático – 1º Batalhão de Guerra Eletrônica.* (Trabalho de Conclusão de Curso) Escola de Comando e Estado-Maior. Rio de Janeiro/Brasil.

Ejército Argentino (2014). ROB -00-01 Conducción para las Fuerzas Terrestre. Buenos Aires/Argentina.

Ejército Brasileño. Estado Mayor del Ejército. (2014). *EB 20-MC 10.213 Operações de Informação*. Brasília/Brasil.

Ejército del Estados Unidos. Headquarters, Department of the Army (2014). *FM 3-38, Ciber Electomagnetic Activities.*Washington, DC.

ESTADOS UNIDOS. United States Cyber Command http://www.arcyber.army.mil/

FERRARI, Bruno, CORNACHIONE Daniella, LOYOLA Leandro. (2011). *A Guerra Virtual*

Começou. Rio de Janeiro/Brasil: Época.

GEE, Alastair. (2009). *El oescuro arte de la ciberguerra.* Manual de Informaciones. Abril – Junio 2009 – Nº 2, Vol LI. P. 36-38

HERNANDEZ, Jorge Lópes. (2013). Capacidades Esesnciales para una Ciberdensa Nacional. CRG- Cibersecurety Researsh Group. INDRA. p.4

LEWIS, A. James. (2010) *Thresholds for Cyberwar*. Center for Strategic and International Studies.

LUCERO, Julio Geraldo. *La dimensión desconocida.* Escuela Superior de Guerra Conjunta. ESGCFFAA. Revista Visión Conjunta Nº 12. p. 41.

MANDARINO Jr, Raphael. (2010). *Segurança e defesa do espaço cibernético brasileiro*. Recife/Brasil: Cubzac.

MANDARINO, Jr Rafael. (2009).*Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro*, Brasília/Brasil.

MANDARINO, Raphael Jr y CANONGIA, Cláudia. (2010). *Livro Verde: Segurança Cibernética no Brasil*. Brasília/Brasil. Ed. ABIN /GSIPR.

Ministério de la Defensa de Brasil. (2014). *Doutrina Militar de Defesa Cibernética*, Brasília, 2014. Recuperado en:

Ministério de la Defensa de Brasil. (2014). *Política Cibernética de Defesa*, Brasília/Brasil. Recuperado en:

Ministerio de la Defensa. (2011). *MD30-M-01, Doutrina de Operações Conjuntas*, 1º Volume. Brasília/Brasil.

MURPHY, Dennis M. (2010). *Atacar ou Defender? Como Explorar as Informações e Equilibrar os Riscos no Ciberespaço*. Militar Review. Ed. Brasileira.

NATO. Corporative Cyber Defense Center Excellence. https://ccdcoe.org/

Poder Ejecutivo de Brasil. (2000). *Decreto Federal Nº 3.505*. Recuperado de:

Poder Ejecutivo de Brasil. (2005). *Decreto Federal Nº 5.484*. Recuperado de:

Poder Ejecutivo de Brasil. (2006). *Decreto Federal Nº* 5.772. Recuperado de:

Poder Ejecutivo de Brasil. (2008). Estratégia Nacional de Defesa, Brasília/Brasil. Recuprado en:

Poder Executivo Nacional. (2005). Decreto Regulador. Nº 378.

Poder Executivo Nacional. (2006). Decreto Regulador Nº 1.691/06. Recuperado en:

Poder Executivo Nacional. (2006). Decreto Regulador Nº 727/06. Recuperado en:

Poder Executivo Nacional. (2009). Decreto 1.714.

Poder Executivo Nacional. (2011). Resolución Nº 580. Recuperado en: http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

Poder Legislativo de Brasil. (1984). *Lei Federal Nº 7.232*. Recuperado de: http://www.planalto.gov.br/ccivil_03/leis/L7232.htm

Poder Legislativo de Brasil. (1988). *Constituição Federal de 1988*. Recuperado de:

Poder Legislativo de Brasil. (2003). *Lei Federal Nº 10.638*. Recuperado de:

Poder Legislativo Nacional. (1998). Ley Nº 24.948.

STEL, Enrique. (2003). *La Guerra Cibernética. El Ciberespacio la cuarta fuerza*. Editorial Dunken.

THOMAS, Timothy. (2009) *Vigilancia Electrónica China de Largo Alcance.* Military Review. Centro de Armas Combinadas USARMY. Marzo – Abril 2009. p. 27.

TOFFLER, Alvin; TOFFLER, Heidi. (1994). *Guerra e Anti-Guerra*. Livros do Brasil, Lisboa.

Universidad Nacional de San Luis. (2013). *Planeamiento Estratégico Informático. Planeamiento Basado en Capacidades Aplicado al Planeamiento Estratégico de la Ciberdefensa*. (7º Simposio Argentino de Informática de Estado). San Luis. Argentina .p. 281

UZAL, Roberto. (2014). *Artículo. ¿Guerra Cibernética: un desafío para la Defensa Nacional?* Revista Visión Conjunta Nº 7. Recuperado de: http://esgcffaa.mil.ar/numero7/40.html. p. 40-42.