MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

TRABAJO FINAL INTEGRADOR

TEMA:

LA GUERRA CIBERNETICA EN UN TEATRO DE OPERACIONES

TÍTULO:

LA GUERRA CIBERNÉTICA EN EL NIVEL OPERACIONAL

AUTOR: Capitán de Eduardo Pablo PÁEZ

PROFESORA: Lic. MARÍA CRISTINA ALONSO

Año 2014

Resumen

El mundo de hoy se ha convertido en un lugar mucho más complejo que antaño. La manera que el ser humano se comunica ha mutado desde el intercambio emisor, medio, receptor, a una modalidad de comunicaciones sin precedentes.

En la actualidad, y por medio de Internet, La red de redes en general involucra a todas las actividades humanas, permite no solo una nueva manera de comunicar sino que a su vez conecta y controla no solo a la persona sino también puntos estratégicos de los países. Existen antecedentes respecto de que, en la forma de música o fotografías de familiares, poderosas Ciber Armas fueron introducidas en redes de computadoras aisladas / preservadas pertenecientes a la infraestructura crítica (muy sensitiva) de determinados países.

Estos hechos deben ponernos en alerta y se requiere por parte de las fuerzas armadas adoptar medidas de prevención y seguridad, dado que se observan deficiencias en ese ámbito, hay que analizar esas deficiencias para tomar medidas permanentes y de carácter dinámico.

El presente trabajo considera la organización y funcionamiento de los distintos servicios de informática de las tres Fuerzas Armadas y la interrelación entre estos y las capacidades para desempeñarse en un escenario virtual para hacer frente a las amenazas en el nivel operacional. La finalidad es establecer una organización de nivel conjunto que permita mantener la capacidad y la efectividad de las operaciones militares en un Teatro de Operaciones en el ámbito de la ciber defensa. SE confirma que "Contar con un comando conjunto para la ciber defensa favorecerá las operaciones dentro de un teatro de operaciones".

Palabras clave:

Ciber defensa- Comando Conjunto- Organización- Nivel Operacional- Teatro de Operaciones

Tabla de Contenidos

Introducción

Se pude definir a la sociedad actual como aquella en la cual predominan las TIC.s que son tecnologías de la información y la comunicación y permite a través de internet y las redes sociales estar conectados en actividades laborales, sociales entre otras.

Por medio de estos recursos tecnológicos, se ha comprobado que bajo la forma de música o fotografías de familiares, poderosas Ciber Armas fueron introducidas en redes de computadoras aisladas / preservadas pertenecientes a la infraestructura crítica de determinados países

Estos hechos ponen en alerta al país y a sus FF.AA. que requiere adopten medidas de prevención y seguridad, dado que se observan deficiencias en ese ámbito, las mismas se deben analizar para tomar medidas permanentes y de carácter dinámico.

Si se tiene en cuenta que el uso de la tecnología por instituciones y la población en los últimos treinta años, el incremento del acceso a internet y la interacción de las denominadas redes, permite que las acciones de guerra, terrorismo, sabotaje y robo de datos que existen entre los estados y otras organizaciones, sean virtuales y se dan en el denominado ciber-espacio.

Como este tema aún no ha sido desarrollado en profundidad, esta investigación es relevante ya que permite abrir nuevos conocimientos sobre el ciber espacio.

La ciberdefensa ha sido tratada con anterioridad, y lo podemos apreciar en los trabajos de Eduardo Llambí[1] (sobre las TIC y su incidencia en el teatro de operaciones), un grupo de académicos de la universidad europea de Madrid[2], en la que enlazan las infraestructuras críticas con las políticas de seguridad, también en el campo de lo concreto, se puede constatar que países como Gran Bretaña, Brasil, la Federación Rusa y estados Unidos, entre muchos otros, han conducido acciones

[1] Llambí, Eduardo Ignacio, Escuela de Guerra Conjunta. "Nuevas Tecnologías de Información y Comunicación (TIC) y su influencia en los teatros de operaciones (TO) modernos", Ciudad Autónoma de Buenos Aires, año 2011.

[2] Carlos Díez Molina, Javier Perojo Gascón, Juan José Penide Blanco, Mikel Arias R. "Ciber-terrorismo Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber-ataques terroristas. Escuela Politécnica de la Universidad Europea de Madrid, 2011

tendiendo a reducir las vulnerabilidades en el ciber espacio. Así también han avanzado en la normativa y la legislación que ampare aquellos actos necesarios para contrarrestar y responder a un ciber ataque. El resultado fue la implementación de sendos comandos cibernéticos. En la actualidad, en trabajos más recientes podemos mencionar a Rubén Silva[3] y Daniel Giudice[4], donde el primero analizó el sistema de seguridad informática para los organismos de la administración pública con el fin de compatibilizarlo con los organismos de las fuerzas armadas, para reducir las amenazas de ataques virtuales. Por otro lado, Giudice planteó que la defensa de la infraestructura y los medios militares en el teatro de operaciones se asegura mediante la capacitación de personal en el área de trabajo de redes.

En el resto del mundo, en la tendencia lidera Estados Unidos y es el primero donde los pensadores estratégicos ya integran las ciber operaciones dentro del marco conjunto y operacional, marcando pautas con el fin de proveer y asegurar la libertad de acción a un comandante de teatro de operaciones. En la región existen otras iniciativas similares: la cumbre sobre la gobernanza de internet Net Mundial Brasil 2014 donde se debatió básicamente el modo en el que se gestiona la Internet. Esto dio origen a diversos simposios en el país, avanzando desde el punto de vista académico y técnico en pos de desarrollar herramientas que den el soporte necesario para hacer frente a las amenazas y desafíos en este campo. El Ministerio de Defensa Argentino, por su lado, decidió crear el Comando de Ciberdefensa, mostrando una voluntad por demás manifiesta en no quedarse atrás en estos menesteres.

Estos antecedentes nos llevan a la siguiente reflexión: ¿cómo debe organizarse un Comando Conjunto de las Fuerzas Armadas para hacer frente a la amenaza de la guerra cibernética?

Si bien los ataques en el campo cibernético se desencadenan tanto sobre objetivos económicos o financieros, como en aquellas infraestructuras que se consideran críticas, el análisis se centrará en nivel operacional y se analizarán las áreas, funciones, herramientas y factores organizacionales que contribuyen a distinguir la conveniencia, ventajas y desventajas para la creación de un Comando Conjunto para

[3] Silva, Rubén Héctor, Escuela de Guerra Naval. "Ataques Virtuales y la seguridad Informática", Ciudad Autónoma de Buenos Aires, año 2013.

[4] Giudice, Daniel Eduardo, Escuela de Guerra Conjunta. "Lineamientos para la seguridad cibernética en un teatro de operaciones", Ciudad Autónoma de Buenos Aires, año 2013.

la ciber defensa. No se profundizará por lo tanto, en aquellas áreas que se consideren ciber crímenes, como la estafa, el lavado de dinero y la utilización de datos personales con fines diversos.

El aporte a la disciplina es proponer crear un Ciber comando conjunto a partir de analizar cuáles son las condiciones que se requiere

El objetivo general de este trabajo es establecer una organización de nivel conjunto que permita mantener la capacidad y la efectividad de las operaciones militares en un Teatro de Operaciones en el ámbito de la ciber defensa.

A los fines de contribuir con el objetivo general, los objetivos específicos se centran en identificar la organización, las funciones y misiones específicas que posee la Armada, la Fuerza Aérea y el Ejército con respecto a la ciber defensa y además en analizar los factores organizacionales intervinientes para materializar un comando conjunto en el ámbito de la ciber defensa.

Como hipótesis se sostiene que contar con un comando conjunto para la ciber defensa favorecerá las operaciones dentro de un teatro de operaciones.

Para este trabajo se utilizará el análisis bibliográfico de la doctrina Argentina, artículos publicados en revistas militares especializadas y artículos de internet en los cuales se trata la problemática en las fuerzas armadas de otros países. La metodología empleada en esta investigación será de tipo exploratoria y descriptiva.

En lo que a la organización del trabajo se refiere, este se divide en tres capítulos en correspondencia con los objetivos anteriormente indicados. En el capítulo 1. Se expone el modo en el cual las diferentes fuerzas encararon la problemática de la ciber defensa. En el capítulo 2, se hará una descripción de los requisitos que podría tener un “ciberguerrero” para desempeñarse en este ambiente novedoso llamado ciberespacio. Finalmente, en el tercer capítulo se detalla una estructura orgánica para la defensa cibernética en un Teatro de Operaciones.

Capitulo Uno

Qué tiene cada quién

1.1. Armada Argentina

Uno de los pilares fundamentales de toda institución de tipo militar es la seguridad y el resguardo de sus activos. Estos van desde los mismos medios con los que se conducen las operaciones como toda aquella información con la cual se planifica, adiestra y opera. El área de la seguridad siempre fue gestionada por los organismos de contrainteligencia, quienes fijaban normas para negarle al enemigo la información propia. Estas normas se aplican tanto a los procedimientos de identificación de las personas, los protocolos de acceso a locales como al manejo de la documentación, con sus distintos niveles de clasificación.

Por otro lado, el estado nacional, en el año 2000 pone en marcha el Plan Nacional de Modernización de la administración pública el cual buscaba medir resultados, mejorar la calidad en las prestaciones, aumentar la eficiencia y efectividad del desempeño público, enfocar la atención al cliente, lograr "transparencia" y otros conceptos similares. Este plan ve la luz con el decreto Nro 103/01 y se encomendó a la Jefatura de Gabinete de Ministros la coordinación de la ejecución de las acciones que se derivaran de dicho plan[5]. En este decreto se aprueba, a su vez, la estructura organizativa de la Secretaría para la Modernización del Estado, de la cual se desprende la Oficina Nacional de Tecnologías de Información. Esta oficina "*implementa las estrategias de innovación informática en la administración pública. Desarrolla sistemas que son utilizados en procedimientos de gestión, fija los estándares que deben utilizar los organismos públicos cuando incorporan nuevas tecnologías, colabora con otras dependencias en la creación de portales informativos y de gestión y promueve la interoperabilidad de las redes de información de las instituciones estatales*[6]". Además busca garantizar la información de la administración pública, "*coordina las respuestas ante los intentos de ataque o*

[5] Decreto 889/2001. Modificación del Decreto Nº 20 de fecha 13.12.1999, en la parte correspondiente a la Subsecretaría de la Gestión Pública, dependiente de la Secretaría para la Modernización del Estado. Transformación del Instituto Nacional de la Administración Pública

[6] Portal de la Secretaría de Gabinete y Coordinación Administrativa. Jefatura de Gabinete de Ministros. Recuperado de: http://www.jefatura.gob.ar/sgp/paginas.dhtml?pagina=27

penetración a las redes informáticas de los organismos públicos, fija los estándares de seguridad y controla que sean cumplidos en los sistemas del Estado[7]"

Es en este contexto que la Armada Argentina adaptó su propia estructura organizacional y creó la Dirección General de Comunicaciones e Informática de la Armada de la cual depende entre otros, el Servicio de Seguridad de la Información.

En el año 2010 se crea el Servicio de Seguridad de Informaciones de la Armada, cuya finalidad se centra en resguardar y preservar la información y todos aquellos sistemas que la gestionen. Se nutre con personal de suboficiales con la especialidad informática cursada en la Escuela de Suboficiales de la Armada durante dos años, que le permiten entre otras cosas, Realizar mantenimiento preventivo, correctivo del equipamiento asignado y de su soporte ya sea de software o hardware y de la conectividad en cada una de las redes. Entender en el desarrollo, diseño y realización de los sistemas necesarios. Implementar y poner en funcionamiento las soluciones. Cubrir puestos orgánicos en los Comandos, Organismos y Dependencias que contemplen el desarrollo de aplicaciones. Conducción / supervisión de personal especializado en Sistemas de Computación de Datos. Diseño y mantenimiento de las aplicaciones que por razones de seguridad le sean asignadas. Realizar tareas en la red de Informática Naval, incluyendo medios físicos de conexión, monitoreo y control, etc.[8] Conocer el marco legal y regulatorio que lo habilitará para desempeñarse adecuadamente en el medio social y técnico que exige a la carrera. Por parte del personal de oficiales, los cursos que se dictan son el Posgrado en análisis de sistemas automatizados de gestión para la defensa, producción y logística y el Posgrado en análisis de sistemas automatizados de gestión para el desarrollo de operaciones militares.

Una vez en el servicio se coordinan diferentes cursos de capacitación de mayores niveles, según las necesidades.

La finalidad ulterior de este servicio es resguardar, puertas adentro, aquellas infraestructuras críticas para el normal funcionamiento de la Armada y el resguardo

[7] Ibidem.

[8] Portal de la Armada Argentina, recuperado en: http://www.essa.ara.mil.ar/CarrerasEscalafones/NavalesIN.html

de la información que fluye por sus redes. Dicta normas y procedimientos y al momento de desarrollar esta investigación no poseen una división de Investigación y Desarrollo.

Tiene un alto grado de interoperabilidad con Fuerza Aérea y Ejército, efectuando intercambio de personal y capacitando, en la escuela técnica del ejército, que dicta cursos y especializaciones de distintos niveles.

1.2. Ejército Argentino

En el Ejército Argentino, su Centro de Ciberdefensa tiene por misión ejecutar Las acciones necesarias para desarrollar las capacidades de Ciberdefensa, Defensa Directa (DD), en el ciberambiente que le compete, a fin de monitorear la infraestructura critica de la información y dar respuesta ante incidentes, tendientes a asegurar el empleo en todo momento de las tecnologías de la información, de las comunicaciones y los sistemas de control inherentes a Instrumento Militar - Fuerza Ejercito, aplicando los conocimientos adquiridos sobre las redes informáticas de la Dirección General Inteligencia[9].

Su dependencia operativa es del Jefe de Estado Mayor General del Ejército y administrativamente depende de la Dirección General de Inteligencia. Con respecto al desarrollo doctrinario, al momento de esta investigación Se han iniciado los estudios preliminares pertinentes (Nivel de ejecución, manuales de procedimientos operativos y los protocolos de empleo, a medida que se evolucione se confeccionarán los documentos definitivos, todo estará sujeto a revisión en esta primera etapa se realizará cada 6(seis) meses, posteriormente una vez al año.

Con respecto al personal del que se nutre, los requisitos para el personal están relacionado con los distintos niveles de la organización: Ingenieros Militares en Informática, Ingenieros civiles en Informática conforman los cuadros superiores. Especialistas en Seguridad Información, en infraestructura y capacitadores. Referido a las políticas de personal civil se realiza una selección entrevistas personales presentación de la documentación que acredite sus conocimientos y aptitudes adquiridas. Una vez seleccionados pasan un período de prueba para confirmarlos posteriormente.

[9] Carbia Federico, Coronel (RE) del Ejército Argentino, Entrevista realizada en septiembre de 2014.

En lo que se refiere a los protocolos de seguridad que utiliza este servicio, los programas que se siguen se basan en las normas ISO27001 sobre seguridad de la información (describe cómo gestionar la seguridad de la información en una empresa, puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande) y la organización que acompaña es la ONTI.

Ya que se está gestando la implementación de medidas de control y monitoreo con la finalidad de poder identificar ataques e incidentes y para luego tener información estadística, no se tienen antecedentes de ciberataques perpetrados contra esta fuerza

Desde el punto de vista de la interacción del Ejército con las otras fuerzas, referido al conocimiento de lo que están realizando las otras fuerzas, hasta el momento no se ha interactuado con las mismas a nivel operativo. A partir de la creación y la puesta en ejecución del comando se presume que existirán fluidos contactos con las mismas.

1.3. Fuerza Aérea Argentina

Al momento de elaboración del presente trabajo, la Fuerza Aérea Argentina se encuentra en las instancias iniciales de una Dirección de Ciberdefensa de la Fuerza Aérea. La misma tiene por misión preservar la infraestructura crítica que se le haya encomendado, para contribuir con el cumplimiento de la misión de la FAA[10].

La Dirección de Ciberdefensa depende orgánicamente del señor Jefe de Estado Mayor General de la Fuerza Aérea, y en su orgánica prevé una dirección con un departamento Planes y Doctrina, un departamento Operaciones y un departamento Apoyo.

Con respecto al personal que conforme la dirección de ciberdefensa, se entiende que el área de recursos humanos constituye el centro de gravedad y factor determinante de la ciberdefensa, en carácter ideal el personal que esté afectado a dichas funciones debiera provenir de áreas tales como Informática, Comunicaciones, Inteligencia, Guerra Electrónica, Operaciones, Asuntos Jurídicos así como personas que hayan obtenido algún tipo de certificación internacional en el área de la

[10] Delpino, Luis Antonio, Comodoro de la Fuerza Aérea Argentina. Entrevista realizada en septiembre de 2014.

seguridad de la información, hacking ético y la forensia informática. Al respecto, el Comodoro Delpino, quien forma parte del equipo de desarrollo de ciberdefensa, indica que "En ciberdefensa, disponer de recursos humanos idóneos nos otorga la libertad de acción suficiente y necesaria para determinar (por propios medios, sin necesidad de asesoramiento externo) aspectos tales como la doctrina (organización y procedimientos) y los recursos tecnológicos que nos permitan alcanzar las aptitudes de ciberdefensa que hayan sido establecidas".

Las políticas de personal son tales que, "tratándose de algo desconocido pero altamente exigente, el inicio de la subcapacidad será llevado adelante con los recursos humanos que se dispongan y no con los recursos humanos ideales. El tiempo y la experiencia extraída permitirán delinear una política de personal para ciberdefensa, tendiendo al concepto de cibercombatientes, ciberguerreros o ciberreservistas[11]".

Desde el punto de vista de la doctrina, al no poseer ninguna por el momento, se espera que dicha doctrina tome forma al combinar experiencia propia con la de otros actores con mayor trayectoria. Por el mismo motivo, ante eventos de ataques informáticos se procede con la experiencia extraída del área de la seguridad informática ya vigente. La base de partida son las políticas y normas establecidas por el organismo responsable de la seguridad informática de la FAA, para que a futuro y en base a la experiencia adquirida se puedan establecer políticas, normas y procedimientos de ciberdefensa. Los activos críticos de la fuerza que se protegen son aquellos cuya afectación podrían poner en riesgo el cumplimiento de la responsabilidad primaria de la FAA (la vigilancia y control del aeroespacio de interés).

Con respecto a la interacción que se tiene con las otras fuerzas, el personal de la FAA interactuó con personal de las otras Fuerzas, durante las reuniones sostenidas para la redacción del Plan Estratégico de Ciberdefensa del Estado Mayor Conjunto y no se ha tenido, en estas primeras instancias del desarrollo de la Dirección de Ciberdefensa, contacto con organismos universitarios.

[11] Ibídem.

1.4. Conclusiones parciales.

Las tres fuerzas armadas se encuentran desarrollando sus centros de ciberdefensa con sus propias fórmulas. Existe una diferencia de dependencia orgánica, según cómo se entiende el manejo de la información; la Armada Argentina, considera a la información como un activo crítico que depende de las Comunicaciones. El Ejército Argentino y la Fuerza Aérea, consideran que este activo depende administrativamente de la Dirección General de Inteligencia (aunque el personal jerárquico de la Armada está orientado en Inteligencia).

De las tres fuerzas, es la Armada Argentina la que tiene mayor trayectoria en el tema, y la Fuerza Aérea es la fuerza que se encuentra haciendo sus primeras experiencias en el campo particular.

Si bien no existe una normalización en la formación y en la organización básica en cada fuerza, las finalidades son las mismas y todas tienen el enorme potencial para nutrir a un Comando Conjunto de Ciberdefensa para que se desempeñe con la flexibilidad necesaria en la complejidad de este nuevo campo de combate denominado “ciberespacio”.

Capitulo dos

El ciberguerrero y el Teatro de Operaciones

2.1. Ámbito de aplicación.

En el campo de batalla virtual llamado ciberespacio, se puede individualizar a aquellos individuos que tomarán acción y que se los puede agrupar dentro de cuatro funciones básicas: "*Operadores de ciberguerra, que planean, dirigen y ejecutan actividades ofensivas y defensivas en y a través del ciberespacio; técnicos del ciberespacio, que proporcionan y mantienen partes asignadas del ciberespacio; analistas y encargados de la selección de objetivos de ciberguerra, que ofrecen apoyo de inteligencia a las operaciones de ciberguerra y finalmente, desarrolladores de ciberguerra, que diseñan y crean herramientas y armas para la ciberguerra*[12]". En el caso de este trabajo, se centra en la ciberdefensa ysi bien se considera que las cuatro funciones básicas se aplican del mismo modo en los tres niveles (Estratégico, Operacional y Táctico), el que particularmente interesa es el Teatro de Operaciones (el nivel operacional).

2.2. Las características del ciber soldado

En este ámbito "*se requiere por parte del personal una especialización detallada y especifica ya que, dentro del ciberespacio y la tecnología cibernética, se pueden encontrar diversos campos de especialización*[13]".

La autora Barrera, M.E. dice que la formación del cibersoldado, se tiene que fundar en "*sólidos conocimientos en informática, electrónica y comunicación; con una adecuada meta-cognición de sus conocimientos, que lo ayudará a desplegar sus habilidades e inteligencia en tiempo real, en un espacio virtual*[14]". Estas características, podrían volcarse hacia aquellos técnicos del ciberespacio. Por otro lado, y enfocándose hacia aquellos sujetos que planifican y dirigen, según Brett T. Williams, a pesar de la complejidad técnica del ciberespacio, un Comandante Conjunto puede y debe dirigir operaciones en el ciberespacio en el nivel operacional usando la doctrina actual y los mismos procesos de planeamiento y ejecución[15].

---

[12] Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012.

[13] Giudice, Daniel "Lineamientos para la seguridad cibernética en un teatro de operaciones" Escuela de Guerra Conjunta. Ciudad Autónoma de Buenos Aires, año 2013

[14] Barrera, Marisa Eugenia "La formación y el perfil del cibersoldado"

[15] Williams T. Brett, " The Joint Force Commander's Guide to Cyberspace Operations". Recuperado

La autora Barrera, M E en un trabajo que guió y cuyo objetivo fue caracterizar las personalidades de los individuos que se desempeñan en el ambiente del ciberespacio, encontró que existen diferencias marcadas entre un soldado de corte tradicional y el denominado cibersoldado: El soldado formado bajo las rígidas convenciones castrenses, es activo, esquemático, retrospectivo, longitudinal, tiene una visión parcial (dado que maneja información según el nivel en el que se encuentra dentro de la cadena de comando), es predecible, tiene una formación básica en informática (como la tiene cualquier usuario normal y corriente) y el teatro de operaciones donde se prepara para actuar se limita a la tierra, el mar y el aire. El cibersoldado en cambio, es proactivo, plástico, prospectivo, transversal, posee una mayor cosmovisión, es impredecible y disruptivo, posee una avanzada capacidad informática y el teatro de operaciones en el que se desempeña es el ciberespacio o espacio virtual[16].

La autora enfoca su análisis desde una perspectiva psicológica y concluye en el perfil de un cibersoldado a partir de tres ejes principales: "*una avanzada capacitación en informática; en la obtención y el manejo de la información y en el poder de análisis de la misma con una concepción táctica y estratégica de su uso*[17]".

Por otro lado, se debe considerar a los llamados "hackers" ("*personas que entran de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo*[18]) desde el punto de vista psicológico, pues permite tener una comprensión de sus prácticas. Se caracterizan por ser transgresores, indisciplinados, obsesivo- compulsivos por acumular conocimientos. Se definen como curiosos, autodidactas e investigan todo lo relacionado con la electrónica y la informática. Sus motivaciones son el dinero y el reconocimiento, si no por todos, por sus pares. No son reservados, necesitan evidenciar y publicar sus logros. Son competitivos y en los estudios no son aplicados pero tienen aptitudes para la tecnología, como se planteó más arriba. Por lo general, esto hace que sus habilidades sociales sean limitadas: se muestran como

---

de: http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/8461/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx.Abril 2014

[16] Barrera, Marisa Eugenia "La formación y el perfil del cibersoldado"

[17] Ibídem.

[18] Castro, Luis "¿Qué es hacker?" recuperado en: http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es-Hacker.htm

extrovertidos o por el contrario, muy introspectivos. Conocer sus características es importante porque hasta que se desarrolle la capacidad técnica necesaria para que una fuerza se desenvuelva en un ambiente cibernético altamente hostil, puede darse la necesidad de contratar uno de estos particulares sujetos, de quienes no puede esperarse un trato similar a una persona formada en el seno de las fuerzas armadas y cuyo manejo y control deberá ser seguido con mucho recaudo.

A continuación y a manera de resumen, se constan las siguientes tablas:

Figura Nro. 1 Características Generales Del Perfil De Un Soldado Tradicional

JERARQUIA	COMPETENCIAS BASICAS	COMPETENCIAS GENERICAS	COMPETENCIAS ESPECIFICAS O TECNICAS	TIEMPO/LUGAR
SOLDADO TRADICIONAL (INTELIGENCIA)	• Valores éticos y morales. Vocación, espíritu de servicio y superación. • Conocimiento específico en Armas (de acuerdo a las FF.AA.) • Adecuado nivel de redacción, comunicación escrita y Comprensión lectora. • Dominio de herramientas Office nivel básico, Word, PowerPoint, Excel. Manejo de internet e intranet. • Adecuado nivel intelectual.	• **Competencias personales**: - Iniciativa - Reservado - Tenacidad - Tolerancia a la frustración. - Estabilidad emocional • **Competencias de liderazgo**: -Toma de decisiones -Trabajo en equipo • **Competencias cognitivas**: - Pensamiento Práctico.	• Capacidad táctica • Manejo de información clasificada. • Adecuada atención y Concentración • Habilidad de planificar a corto, mediano y largo plazo • Capacidad organizadora	**TRANSCURRE EN UN DETERMINADO TIEMPO/ESPACIO (tierra, mar o aire)** Lic. Marisa Barrera

Fuente: Barrera, Marisa Eugenia. Apuntes de clase. Armada Argentina

Figura Nro. 2 Características Generales Del Perfil De Un Cibersoldado

JERARQUIA	COMPETENCIAS BASICAS	COMPETENCIAS GENERICAS	COMPETENCIAS ESPECIFICAS O TECNICAS	TIEMPO/LUGAR
CIBERSOLDADO	• Valores, vocación, espíritu de servicio y superación. • Conocimiento específico en Armas (de acuerdo a las FF.AA.) • Adecuado nivel de redacción, comunicación escrita y lectora. • Capacidad de adquirir nuevos conocimientos. • Alta capacitación en Informática.(expertos en programas y protocolos) • Compromiso Institucional.	• **Competencias personales**: - Proactivo - Reserva/Discreción - Tenacidad - Tolerancia a la frustración - Estabilidad emocional. • **Competencias de liderazgo**: -Toma de decisiones -Trabajo en equipo -Trabajo individual. • **Competencias cognitivas**: -Pensamiento Analítico, orientado a la formación continua.	• Capacidad táctica, estratégica y operacional • Manejo de información clasificada. • Adecuada atención y Concentración distribuida • Adecuado Nivel de Manejo y comprensión de la TIC. • Tolerancia al estrés ante la ambigüedad de incertidumbre y riesgo. • Capacidad de creatividad innovación y alta competitividad • Capacitación permanente.	**TRANSCURRE EN TIEMPO REAL (espacio virtual)** Lic. Marisa Barrera

Fuente: Barrera, Marisa Eugenia. Apuntes de clase. Armada Argentina

2.3.El ciberespacio y el nivel operacional

Si se considera al teatro de operaciones como aquel territorio, tanto propio como enemigo, necesario para el desarrollo de operaciones militares en el nivel estratégico operacional[19], 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*[20]*"*.

Además, hay que tener en cuenta que un ataque cibernético puede ser conducido a través de espacios virtuales de gente común, de empresas, de instituciones o naciones que incluso no saben que están siendo parte del enrutamiento 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.

[19] RFD–99–01. Terminología Castrense de uso en el Ejército Argentino. CD - 01. Edición Año 2002.

[20] Sten, Enrique. La guerra cibernética el ciberespacio - la cuarta fuerza Editorial Dunken

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 ni siquiera es 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 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[21]. 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*[22]".

2.4. La formación de los cibersoldados

Las particularidades del este ámbito obliga a los especialistas dedicados a desenvolverse en un ambiente de ciberdefensa a contar con un conjunto de pericias, que les permita establecer, monitorear y proyectar, cuando sea necesario, el poder de combate en el ciberespacio. Estos deben saber sobre desarrollo y programación de software. De esta manera se lograría cubrir el espectro completo de tareas que

[21] Williams T. Brett, "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 2014

[22] Ibídem

pudieran presentarse en un Teatro de Operaciones tales como son: la preparación, la ejecución y la supervisión de las acciones[23].

Los cibersoldados necesitan poseer un íntegro conocimiento de las tecnologías que inciden y que pueden emplearse para su accionar, teniendo en cuenta la importancia vital que implica la salvaguarda de la información. No obstante, el ciberespacio, como los otros dominios donde los profesionales de la defensa se desempeñan, 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[24].

Daniel Giudice, asegura que la formación del personal, independientemente de su accionar en el ámbito de la defensa o seguridad, dentro del Teatro de Operaciones o en organizaciones que administren u operen infraestructura sensible a un ataque cibernético, es recomendable tener en cuenta que para integrar la estructura orgánica y áreas de seguridad cibernética de la defensa, tiene que pasar por un riguroso proceso de selección y considera que como mínimo las siguientes acreditaciones para oficiales superiores, oficiales jefes y oficiales subalternos, deben tener una formación académica en el grado en Ingeniería, preferentemente especializados en las áreas sistemas, informática, electrónica y de software. Maestría en disciplina a fin acreditada por la Comisión Nacional de Evaluación y Acreditación Universitaria. Especialización en administración y seguridad informática.

Para el personal de Suboficiales, lo deseable es que cuenten con formación académica en el grado de Técnico Electrónico o Informático, además de una formación en administración y mantenimiento de redes informáticas[25].

2.5. Conclusiones—parciales

Las fuerzas armadas se dedican a la capacitación de su personal con

[23] Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012.

[24] Williams T. Brett, "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 2014

[25] Giudice, Daniel, "Lineamientos para la seguridad cibernética en un Teatro de Operaciones" Escuela de Guerra Conjunta. Ciudad de Buenos Aires, año 2013.

determinadas carreras de grado y de posgrado que tienen que ver con la temática de la ciberdefensa.

Es preciso integrar a los oficiales que se desempeñen en el ciberespacio desde el inicio de su carrera de formación, debiendo poseer las aptitudes psicofísicas, nivel intelectual y vocación militar acorde a las exigencias propias de las operaciones en el ambiente particular.

Los conceptos de Teatro de Guerra y Teatro de Operaciones deben ser revisados y actualizados conforme a la existencia del espacio cibernético, estableciendo parámetros de integración los que a su vez los delimiten adecuadamente.

El proceso de planeamiento de una operación cibernética no tiene grandes diferencias con respecto al proceso de planeamiento tradicional, aplicado a cualquier otro tipo de operación.

El perfil de carrera del conductor especialista en ciberdefensa tiene que ser similar al de comunicaciones, con una formación parecida a los oficiales especialistas en Guerra electrónica y en análisis de sistemas. Es conveniente que los oficiales completen su formación en los cursos de estado mayor, tanto nivel uno como el nivel dos, y que de ser necesario, se capacite al personal en aquellas especialidades necesarias para comprender los pormenores de la gestión de la información y de la seguridad de la misma.

El perfil del cibersoldado tiene diferencias con respecto al soldado tradicional. En una organización inserta en la institución militar, aquellos quienes conduzcan las operaciones deben ser militares orientados con las particularidades técnicas y quienes ejecutan las acciones deben tener una formación más orientada a la técnica. Dado el caso que se deba buscar como recurso a los denominados “hackers”, se debe tener en cuenta a sus esquemas de fidelidad.

Capítulo 3

En este capítulo se desarrollan características de una estructura para la defensa cibernética en un teatro de operaciones

3.1. El campo de batalla virtual

Como se mencionó en el capítulo anterior, las definiciones de Teatro de Operaciones se vuelven ambiguas cuando se habla del ciberespacio. Mientras una fuerza puede ser pensada, organizada, enviada a un teatro de operaciones y sostenida por el tiempo que sea necesario, para alcanzar los objetivos de la campaña, los ciberguerreros no son desplegados en el terreno. Las redes informáticas conectan instantáneamente al mundo entero y muchas infraestructuras consideradas críticas están al alcance de un teclado. Se propone en este trabajo que la organización que se considere, se desempeñará al servicio del Comandante del Teatro de Operaciones. Esto implica que el ámbito de aplicación se limitará a resguardar los sistemas e infraestructuras críticas necesarias para llevar a cabo las operaciones.

3.2. Comandos Conjuntos Funcionales

Según la reglamentación conjunta se denomina al Comando Conjunto Funcional a aquél que se compone por efectivos de por lo menos dos fuerzas armadas que deben operar en el mismo ambiente sobre un aspecto específico de la misión asignada[26]. También se define al Estado Mayor como el grupo que compone una organización militar que tiene por principal función "proporcionar principalmente asesoramiento y asistencia al Comandante en el ejercicio de sus funciones operacionales, de los diversos apoyos, control y gobierno. Es en esencia el órgano de conducción del Comandante[27]".

Ambas acepciones son lo necesariamente flexibles como para aplicarse en casos donde se incursione en campos considerados poco ortodoxos como el que ocupa este trabajo: el ciberespacio.

3.3. Tareas y capacidades

El requerimiento principal de un comandante de teatro de operaciones para

[26] MC 20-01, Manual de Estrategia y Planeamiento para la Acción Militar Conjunta Nivel Operacional- La Campaña. Revisión Edición año 2013

[27] RFD–99–01. Terminología Castrense de uso en el Ejército Argentino. CD - 01. Edición Año 2002.

asegurar su libertad de maniobra es el comando y control. El flujo sin interrupción de información y de datos para los sistemas de armas, o la colección y el análisis de información se apoya en el ciberespacio[28]. Es necesario que el personal adquiera los conocimientos y habilidades para desenvolverse apropiadamente a través de redes y debe comprender cabalmente cómo se ve comprometido el comando y control en el teatro de operaciones si se cede el uso del espectro cibernético al oponente. Por ello, la estructura orgánica de un Comando Conjunto de ciberdefensa debe poner énfasis en lograr la familiarización de profesionales con el espectro completo de amenazas a los sistemas de información y las consiguientes respuestas a los posibles ataques.

La integración de una red de comando y control con las unidades desplegadas en el teatro de operaciones ayuda tanto a la conectividad como a la toma de decisiones y la habilidad para imponer el ritmo en cómo se llevan a cabo las operaciones y su nivel efectividad[29].

Giudice[30] en su investigación acerca de la seguridad cibernética en un teatro de operaciones, enumeró algunas capacidades que resultan útiles en el presente trabajo. Según su opinión, mediante la adquisición y desarrollo de dichas capacidades se puede coadyuvar a la formación de una sólida agencia de ciberdefensa:

• Capacidad de detección, localización e identificación de ciberarmas
• Capacidad de análisis y seguimiento del flujo de redes
• Capacidad de desarrollo e implementación de ciberarmas
• Capacidad de respuesta ante transgresiones a la seguridad de la información
• Capacidad de para evitar el uso del territorio nacional como escenario para perpetrar ciberataques.
• Capacidad para auditar los niveles de seguridad de los sistemas de información de la defensa y de aquella infraestructura critica
• Capacidad para desarrollar y emplear herramientas de criptografía y criptoanálisis nacionales

[28] Williams T. Brett, "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 2014

[29] Salmerón, Rubén Benedicto. "Teorías y conceptos para entender formas actuales de hacer la guerra". Universidad Autónoma de Barcelona.

[30] Giudice, Daniel, "Lineamientos para la seguridad cibernética en un Teatro de Operaciones" Escuela de Guerra Conjunta. Ciudad de Buenos Aires, año 2013.

• Capacidad de interoperabilidad, cooperación y colaboración con otras agencias gubernamentales o que tengan a su cargo la administración de infraestructura critica.
• Capacidad de generar proyectos educativos que se orienten a la formación de profesionales en el área cibernética[31]

Las capacidades enumeradas, son parte de lo que distintos autores centran como principales tareas por parte de un comando cibernético y las agrupan en las siguientes: defender las redes de información; apoyar a los comandantes en el Teatro de Operaciones y defensa contra un ataque cibernético.

Williams en su trabajo, por ejemplo, se centra en la libertad de maniobra y en poder proyectar la fuerza a través del ciberespacio, con el fin de alcanzar los objetivos de la campaña y engloba en tres a las operaciones en el ciberespacio, a saber:

- operaciones de información en la red
- operaciones de ciberdefensa
- operaciones ofensivas en el ciberespacio[32]

La finalidad de las operaciones de información en la red es la de proveer libertad de maniobra para que el comandante de teatro de operaciones consiga información, pueda gestionarla y pueda usarla del mejor modo posible para poder tomar mejores y más rápidas decisiones que el oponente. Williams define a las operaciones de ciberdefensa como aquellas actividades activas y pasivas que permiten superar a un adversario: el énfasis está en cambiar la situación de ventaja que tenga el oponente y retomar la iniciativa. El comando de ciberdefensa tiene que detectar, analizar y mitigar las amenazas, incluso las amenazas internas. Las operaciones ofensivas son aquellas necesarias para lograr un efecto determinado sobre el oponente. Pueden aplicarse a los sistemas de comando y control, como a aquellos sistemas de armas que funcionen en red[33].

[31] Ibídem.

[32] Williams T. Brett, "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 2014

[33] Ibidem.

Para desarrollar las acciones antes mencionadas, se debe tener en cuenta al personal técnico necesario que instala, configura y mantiene los equipos, computadoras, redes y software[34].

3.4. Misión de un Comando Conjunto de Ciberdefensa

Teniendo en cuenta los aspectos y pormenores mencionados hasta ahora, se puede tener una idea global del propósito o razón de ser del comando conjunto de ciberdefensa, que en el caso del presente trabajo está en función de un comandante de teatro de operaciones, al cual tiene que satisfacer sus requerimientos desde la óptica del ciberespacio, el cual si bien no tiene límites, en el presente caso se lo limita al teatro de operaciones. Vale decir, en un tiempo y un lugar determinado.

La misión del Comando Conjunto de Ciberdefensa buscará, según lo anteriormente analizado, garantizar el libre acceso al ciberespacio, como situación necesaria para poder desarrollar las operaciones; establecer un ámbito seguro en el ciberespacio, para garantizar la confidencialidad, disponibilidad e integridad de la información, tanto almacenada, la transmitida o la que está en proceso. Finalmente, obtener y mantener la superioridad en el ciberespacio, durante las operaciones.

Por lo expuesto se define entonces, que la misión del Comando Conjunto de Ciberdefensa es:

Controlar y proteger el ciberespacio propio de las amenazas y acciones cibernéticas del enemigo, para proporcionar seguridad a la propia fuerza y garantizar el comando y control del comandante del teatro de operaciones a fin de asegurar su libertad de acción.

3.5. La organización

La organización del comando conjunto de ciberdefensa debiera estar integrada por personal de las tres fuerzas, los siguientes grupos:

Un estado mayor para elaborar planes, directivas y doctrina. El estado mayor dará al comandante del teatro de operaciones las apreciaciones desde el punto de vista de

[34] Franz, Timothy. “El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación”. Air & Space Power Journal en Español. 2012.

la ciberdefensa y asesorará sobre las acciones a tomar para la solución de un problema militar determinado. Elaborará el anexo "Ciberdefensa" en el plan de campaña.

Un Departamento de Operaciones, que englobe los elementos de defensa, a saber:

- División Monitoreo: a través de aplicaciones y medios físicos, con los cuales se verifica el flujo de datos en la red. Uno de los puntos que suscita mayor controversia a nivel mundial, es precisamente el monitoreo de las actividades en la red, ya que se considera que puede darse la vulneración del derecho a la privacidad. El monitoreo propuesto no analiza los datos en sí, sino que analiza el incremento de dicho flujo y hacia dónde se dirige. La detección de un flujo anómalo dirigido hacia un sistema emparentado a una infraestructura crítica, es la clave para determinar que ese sistema está siendo sometido a un ciberataque.

- División Forensia: analiza la actividad a través de herramientas que permiten a los expertos rastrear y determinar el origen de ciberataques, lo cual es de suma importancia para identificar a los perpetradores y discernir si se trata de particulares o de un estado. La forensia informática es la "*aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal*[35]". Estos procesos legales son necesarios para poder presentar en caso de ser necesario, las pruebas necesarias ante las Naciones Unidas, por ejemplo, en ocasión de demostrar que se ha sido víctima de un ataque por parte de otro estado.

- División Ejecución de Operaciones: es el elemento encargado de ejecutar aquellas acciones ofensivas que garanticen el uso del espectro cibernético para la propia fuerza, con el fin de que el comando y control esté asegurado. "*También tendrá a su cargo replicar un ataque, aplicando técnicas de engaño, trampas de red y el uso de nombres para servidores que con intención buscan ser engañosos. No obstante, es necesario que el personal abocado al ambiente de guerra y con puestos de responsabilidad sea capaz de encaminar con celeridad las comunicaciones de la propia fuerza a rutas secundarias y terciarias, en aquellas ocasiones donde se*

[35] Gómez, Luis Ángel, "La informática forense, una herramienta para combatir la ciberdelincuencia", Ministerio de Seguridad, recuperado de: http://www.minseg.gob.ar/node/1050

pudieran perder los enlaces y nodos y, redireccionar los ataques proyectados por el enemigo hacia rutas sin salida[36]*".*

Como un ataque puede degradar la red, pero no necesariamente colapsarla, es importante poder detectar el punto de ingreso del ataque es decir, "*decidir cuándo y dónde se puede soportar una perturbación al sistema la red, Es vital por otra parte poder detectar en donde la red apoya a la misión*[37]".

- División Coordinación y Enlace: es el elemento que coordina y gestiona los enlaces requeridos tanto entre las fuerzas como también aquellos organismos civiles, universidades y personas que por sus condiciones y habilidades que se los incorpore.

A continuación, un Departamento Investigación y Desarrollo: es el elemento encargado de diseñar el software necesario para ejecutar acciones ofensivas cuando las mismas se requieran, en un marco de legitimidad y en razón de apoyar otras acciones militares, las que deberán buscar de alcanzar los objetivos de la campaña.

Un Departamento Asesoría Jurídica que entienda de los asuntos legales, el cual debe tener un alto grado de interacción con la División forensia Informática. Al momento, sobre la materia existe el manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética, El documento, se ocupa de definir el concepto de ciberguerra, las legítimas razones que un Estado tiene para entrar en ella, y el modo ajustado a derecho de comportarse en la misma, hace especialmente evidente su continuismo en las definiciones de uso de la fuerza, legalidad y legitimidad en el uso de la fuerza, amenaza, legítima defensa, necesidad y proporcionalidad[38].

Un Departamento de Gestión de Activos, donde se realicen las acciones necesarias en función del correcto uso de las redes y la seguridad de la información. Una forma de asegurar la transferencia de información y evitar las vulnerabilidades y filtraciones o fuga de información, puede ser a través de la separación de las redes empleadas dentro del Teatro de Operaciones. De este departamento dependen:
- División Auditoria de Sistema: es el elemento que hace las veces de "equipo

[36] Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012

[37] Ibídem.

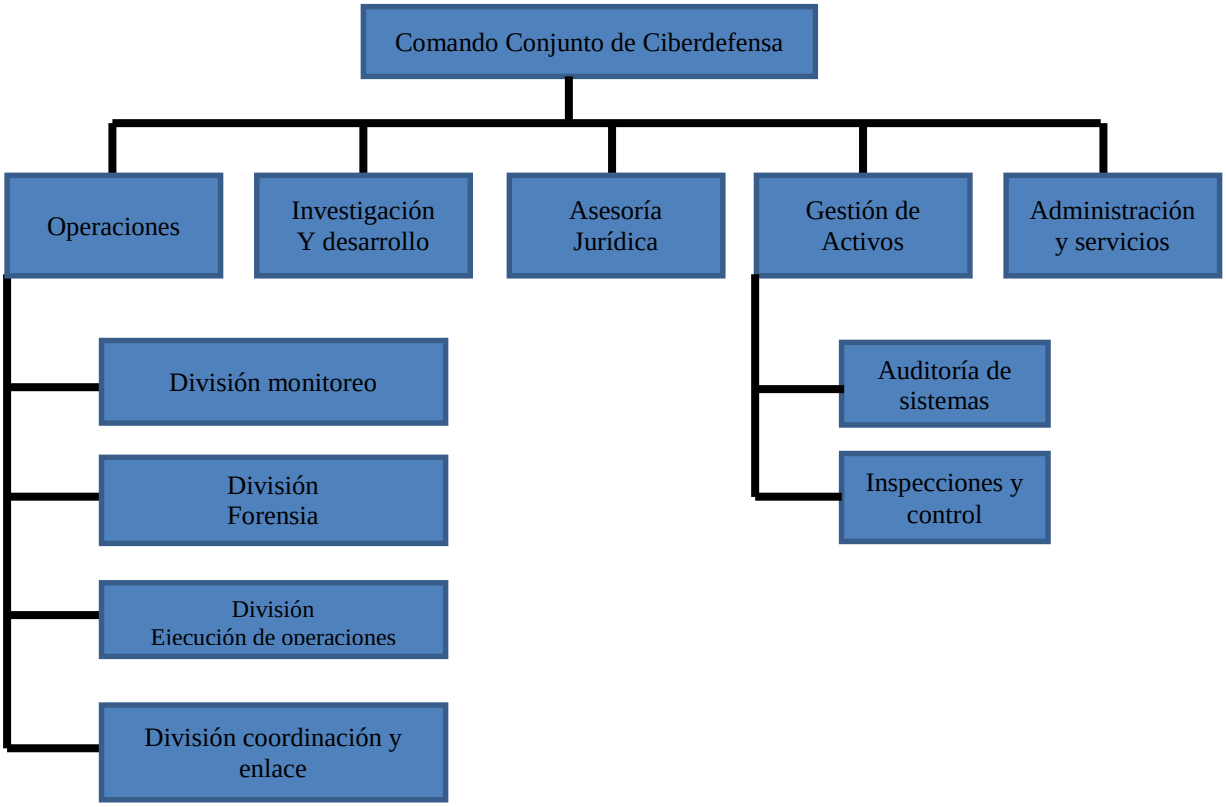
[38] Manual de Tallin sobre el Derecho Internacional Aplicable a la Guerra Cibernética

contrario”; busca las debilidades y trata de explotarlas con el fin de fortalecer el sistema y probar los elementos de monitoreo.

- División Inspecciones y Control: es el elemento a través del cual se verifica que se cumplan las normas de seguridad en el manejo de la información y que no se haga un uso indebido de las redes de informática

Por último un Departamento Administración y Servicios, como encargado de llevar adelante el esfuerzo administrativo, los recursos y las finanzas.

Figura Nro. 3 Organigrama Del Comando Conjunto De Ciberdefensa



Fuente de versión propia, basado en el análisis de los factores desarrollados a lo largo del presente trabajo.

3.6. Conclusiones parciales

Luego de desarrollar este capítulo, se pueden obtener las siguientes conclusiones:

Dado el alcance global que tiene el ciberespacio, un comando conjunto de ciberdefensa encuentra su ámbito de aplicación en la información y las infraestructuras críticas que tengan algún impacto sobre la fuerza desplegada en un teatro de operaciones.

La reglamentación vigente admite y alienta la creación de comandos conjuntos funcionales. Por lo tanto, un comando conjunto de ciberdefensa, es aceptado.

Las tareas y capacidades que se asocian a un comando conjunto de ciberdefensa deben buscar garantizar el libre acceso, establecer un ámbito seguro y obtener y mantener la superioridad en el ciberespacio durante las operaciones para que el comandante operacional mantenga su comando y control y conduzca a sus fuerzas en la campaña.

4. Conclusiones

La investigación arribó a las siguientes conclusiones:

Del capítulo uno las conclusiones parciales son:

Las tres fuerzas armadas se encuentran desarrollando sus centros de ciberdefensa con sus propias fórmulas. Existe una diferencia de dependencia orgánica, según cómo se entiende el manejo de la información; la Armada Argentina, considera a la información como un activo crítico que depende de las Comunicaciones. El Ejército Argentino y la Fuerza Aérea, consideran que este activo depende administrativamente de la Dirección General de Inteligencia (aunque el personal jerárquico de la Armada está orientado en Inteligencia).

De las tres fuerzas, es la Armada Argentina la que tiene mayor trayectoria en el tema, y la Fuerza Aérea es la fuerza que se encuentra haciendo sus primeras experiencias en el campo particular.

Si bien no existe una normalización en la formación y en la organización básica en cada fuerza, las finalidades son las mismas y todas tienen el enorme potencial para nutrir a un Comando Conjunto de Ciberdefensa para que se desempeñe con la flexibilidad necesaria en la complejidad de este nuevo campo de combate denominado “ciberespacio”.

En relación al cap. 2 sus conclusiones parciales son:

Las fuerzas armadas se dedican a la capacitación de su personal con determinadas carreras de grado y de posgrado que se relacionan con la temática de la ciberdefensa.

Es preciso integrar a los oficiales que se desempeñen en el ciberespacio desde el inicio de su carrera de formación, debiendo poseer las aptitudes psicofísicas, nivel intelectual y vocación militar acorde a las exigencias propias de las operaciones en el ambiente particular.

Los conceptos de Teatro de Guerra y Teatro de Operaciones deben ser revisados y actualizados conforme a la existencia del espacio cibernético, estableciendo parámetros de integración los que a su vez los delimiten adecuadamente.

El proceso de planeamiento de una operación cibernética no tiene grandes diferencias con respecto al proceso de planeamiento tradicional, aplicado a cualquier otro tipo de operación.

El perfil de carrera del conductor especialista en ciberdefensa tiene que ser similar al de comunicaciones, con una formación parecida a los oficiales especialistas en Guerra electrónica y en análisis de sistemas. Es conveniente que los oficiales completen su formación en los cursos de estado mayor, tanto nivel uno como el nivel dos, y que de ser necesario, se capacite al personal en aquellas especialidades necesarias para comprender los pormenores de la gestión de la información y de la seguridad de la misma.

El perfil del cibersoldado tiene diferencias con respecto al soldado tradicional. En una organización inserta en la institución militar, aquellos quienes conduzcan las operaciones deben ser militares orientados con las particularidades técnicas y quienes ejecutan las acciones deben tener una formación más orientada a la técnica. Dado el caso que se deba buscar como recurso a los denominados “hackers”, se debe tener en cuenta a sus esquemas de fidelidad.

Por último en el capítulo 3:

Dado el alcance global que tiene el ciberespacio, un comando conjunto de ciberdefensa encuentra su ámbito de aplicación en la información y las infraestructuras críticas que tengan algún impacto sobre la fuerza desplegada en un Teatro de Operaciones.

La reglamentación vigente admite y alienta la creación de comandos conjuntos funcionales. Por lo tanto, un comando conjunto de ciberdefensa, es aceptado.

Las tareas y capacidades que se asocian a un comando conjunto de ciberdefensa deben buscar garantizar el libre acceso, establecer un ámbito seguro y obtener y mantener la superioridad en el ciberespacio durante las operaciones para que el comandante operacional mantenga su comando y control y conduzca a sus fuerzas en la campaña.

Se puede incluir a estas conclusiones ventajas y desventajas de un Comando Conjunto de Ciberdefensa como el propuesto:

Los siguientes factores organizacionales son una ventaja:

- Una Misión clara y acorde, establecida en función a las necesidades de un Comandante de Teatro de Operaciones

- Capacitaciones acordes a la exigencia del campo de la ciberdefensa mediante cursos, especialidades y carreras de grado. No obstante, debe implementarse una carrera con la especialidad ciberdefensa en las tres fuerzas.

- Estructura organizacional flexible y adaptable a las necesidades, avalada por la doctrina.

- Organización conformada con personal de las distintas fuerzas consolida el concepto de trabajo conjunto y asegura la interoperabilidad

Los siguientes factores organizacionales son una desventaja:

- Inexistencia de doctrina propia específica en ciberdefensa

Se puede afirmar, que los objetivos se cumplieron a lo largo del trabajo y también se mostró la validez de la hipótesis planteada, sobre la importancia de contar con un Comando Conjunto de Ciberdefensa; que se desempeñe con acciones que aseguren el apoyo al Comandante del Teatro de Operaciones, preservando asimismo las infraestructuras críticas y el intercambio de datos e información desde el enfoque particular del ciberespacio a través de una organización acorde, nutrida con personal de las tres fuerzas.

Recomendaciones finales

Es conveniente incorporar a los distintos ejercicios de planeamiento el tema de la ciberdefensa. Tanto en ejercicios de planeamiento de gabinete como en ejercicios de planeamiento con el empleo de medios. Se requiere diseñar ejercicios específicos de ciberdefensa para ser aplicados en un teatro de operaciones virtual

Si bien diversos autores manifiestan que la doctrina conjunta existente se acomoda a las operaciones del ciberespacio, se recomienda verificar esta aseveración en base a la práctica y diseño de ejercicios como los recomendados anteriormente.

También se recomienda explorar, como líneas futuras de investigación, el diseño del perfil de carrera para personal de oficiales y de suboficiales con la orientación en operaciones cibernéticas.

Implementar la especialidad de Ciberdefensa/ ciberoperaciones a los institutos de formación.

Anexo 1

Protocolo para Plan de entrevistas

Objetivos de la entrevista:

Determinar de qué manera cada una de las Fuerzas Armadas trata la problemática de la ciberdefensa.

Objetivo secundario:

Saber cómo está organizada la ciberdefensa en la fuerza particular (Armada, Ejército, Fuerza Aérea)

Introducción

Se solicita completar el siguiente cuestionario que se refieren al modo en que su Fuerza trata el particular tema de la ciberdefensa. La distribución del trabajo se compone de tres capítulos: el primero describe lo que tiene y cómo se organiza cada fuerza, el segundo hace una descripción del "ciberguerrero" y un último capítulo donde se diseña finalmente, un comando conjunto de ciberdefensa que se desempeñe para apoyar al Comandante de Teatro en un conflicto dado.

Tópico 1: Organización

- ¿Existe una organización dedicada a la ciberdefensa?
- ¿Determinar cuál es la misión de la organización que exista
- ¿Cómo es la orgánica?

Tópico 2: Doctrina

- ¿Existe doctrina al respecto?
- De no existir doctrina ¿cómo se procede y de acuerdo con qué?
- ¿Existe algún tipo de regulación para las operaciones de ciberdefensa?
- ¿Desde la organización particular se emanan políticas de seguridad? ¿De qué forma se encaminan?

Tópico 3: Operaciones

- Saber a qué nivel se maneja la ciberdefensa de la fuerza particular (¿Quién conduce las acciones de ciberdefensa?)
- ¿En qué medida la fuerza particular contribuye al comando conjunto de ciberdefensa?
- ¿A qué se consideran activos críticos a proteger?
- ¿Se trabaja con algún protocolo de seguridad o algún programa?
- ¿Se tienen antecedentes de ciberataques de los que se ha sido víctima o si se ha actuado para impedir algún ataque en progreso?

Tópico 4 Personal

- ¿Cuáles son los requisitos del personal para integrar la organización de ciberdefensa?
- ¿Cómo son las políticas de personal?

Tópico 4 Interacción:

- ¿Se sabe algo al respecto de las otras fuerzas?
- ¿Tiene algún grado de interacción con las otras fuerzas?
- ¿Existe interacción con universidades, organizaciones civiles o gubernamentales?

Las preguntas que se envían están destinadas a conformar el primer capítulo. Cualquier otra consideración que se le ocurra que pueda aportar, será bien recibido.

Muchas gracias por su colaboración.

Apéndice Alfa al Anexo1

TOPICO 1: ORGANIZACIÓN			
RESP.	ENTREVISTADO UNO	ENTREVISTADO DOS	ENTREVISTADO TRES
UNO	SÍ	SI	SI
DOS	La finalidad ulterior de este servicio es resguardar aquellas infraestructuras críticas para el normal funcionamiento de la Armada y el resguardo de la información que fluye por sus redes	El Ejército Argentino ejecutará las acciones necesarias para desarrollar las capacidades de Ciberdefensa, Defensa Directa (DD), en el ciberambiente que le compete, a fin de monitorear la infraestructura critica de la información y dar respuesta ante incidentes, tendientes a asegurar el empleo en todo momento de las tecnologías de la información, de las comunicaciones y los sistemas de control inherentes a Instrumento Militar - Fuerza Ejercito, aplicando los conocimientos adquiridos sobre las redes informáticas de la Dir. Gral. Icia.	La Dirección de Ciberdefensa de la FAA deberá preservar la infraestructura crítica que se le haya encomendado, para contribuir al cumplimiento de la Misión de la FAA.
TRES	Es en este contexto que la Armada Argentina adaptó su propia estructura organizacional y creó la Dirección General de Comunicaciones e Informática de la Armada que depende	La dependencia operativa del Centro de Ciberdefensa del EA es del JEMGE y administrativamente depende de la Dir. Gral. Icia	Prevé una Dirección con un Departamento Planes y Doctrina, un Departamento Operaciones y un Departamento Apoyo; con dependencia orgánica del señor JEMGFAA.
TOPICO 2: DOCTRINA			
RESP.	ENTREVISTADO UNO	ENTREVISTADO DOS	ENTREVISTADO TRES
UNO	NO	NO	En algo desconocido la misma no existe, ella irá tomando forma de combinar la experiencia propia con la experiencia de otros actores.
DOS	Se usan las “mejores prácticas” que sugiere la ONTI y normas propias que se promulgaron para seguridad informática	Se han iniciado los estudios preliminares pertinentes (NIVEL DE EJECUCIÓN, Manuales de Procedimientos Operativos y los Protocolos de empleo, a medida que se evolucione se confeccionarán los documentos definitivos, todo estará sujeto a revisión en esta primera etapa se realizará cada 6(seis) meses, posteriormente una vez al año	Entendemos que al inicio se procederá con la experiencia que la FAA haya extraído en el área de la seguridad informática (incidentes informáticos).
TRES	Se siguen procedimientos según los que seguiría un CSIRT (un equipo de respuestas a emergencias informáticas)	Si existen. Las Operaciones Complementarias de Ciberdefensa solo están contempladas para la ejecución de la Ciberdefensa Directa (Defensa). Las operaciones de Ciberdefensa Indirecta (Ataque), solo deberán ser ejecutadas por orden directa del PEN.	Entendemos que al inicio se procederá con la experiencia que la FAA haya extraído en el área de la seguridad informática (incidentes informáticos).

CUATRO	las políticas de seguridad informática ya estaban establecidas en la Armada con la creación del servicio de seguridad de informaciones de la Armada	En la organización sigue las recomendaciones de la ISO27001 (ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.) , ISO27002 y la implementación de tecnología en basadas bajo las buenas prácticas en seguridad	En un principio la base de partida serán las políticas y normas establecidas por el organismo responsable de la seguridad informática de la FAA, para a futuro y en base a la experiencia adquirida establecer políticas, normas y procedimientos de ciberdefensa.

TÓPICO 3 OPERACIONES			
RESP.	ENTREVISTADO UNO	ENTREVISTADO DOS	ENTREVISTADO TRES
UNO	depende directamente del Jefe de Estado Mayor General de la Armada	La dependencia operativa del Centro de Ciberdefensa del EA es del JEMGE y administrativamente depende de la Dir. Gral. Icia	Una vez logradas todas las aptitudes, la conducción de dichas acciones estarán a cargo del Departamento Operaciones de la Dirección de Ciberdefensa.
DOS	El Comando Conjunto es un órgano coordinador, cuando tiene que armar una operación, los tres Estado Mayores le dan las cosas que requiere.	El Comando Conjunto de Ciberdefensa es autoridad de coordinación sobre los CERTs de cada FFAA. Todos los incidentes de Ciberdefensa deben ser reportados a ese Comando y también al arCERT de la ONTI (Oficina Nacional de Tecnologías de Información) responsable de la Ciberdefensa a nivel de la Administración Pública Nacional	En ciberdefensa la cooperación es elemental y determinante, en estas instancias iniciales de implementación ambos –la FAA y el Comando Conjunto de Ciberdefensa- mantienen un diálogo y coordinación constantes, habiendo destinado un Oficial Superior con cambio de destino a dicho organismo conjunto.
TRES	Como activo crítico se considera a la información bajo cualquiera de sus acepciones. Pueden ser información clasificada, al igual que las comunicaciones en forma de voz, datos o video	Los activos críticos de una organización son los activos con mayor nivel de criticidad que puede tener una organización, que en caso de verse comprometidos o no funcionales tienen el mayor grado de perjuicio para la misma. Para establecer el grado de criticidad de los activos se realiza por medio del estudio de análisis de riesgo.	Por “activos críticos de la fuerza” deben entenderse aquellos cuya afectación podrían poner en riesgo el cumplimiento de la responsabilidad primaria de la FAA (la vigilancia y control del aeroespacio de interés).
CUATRO	se trabaja según protocolos establecidos de seguridad informática, basados en recomendaciones de la ONTI	El programa que seguimos es base a la ISO27001 sobre seguridad de la información, y la organización que acompaña es la ONTI.	Entendemos que al inicio se procederá con la experiencia que la FAA haya extraído en el área de la seguridad informática (incidentes informáticos).
CINCO	se han detectado intrusiones, pero no se vio afectado ningún sistema	No se tienen antecedentes porque está gestando la implementación de medidas de control y monitoreo con la finalidad de poder identificar ataques e incidentes y para luego tener información estadística.	Las respuestas de la FAA en este sentido han sido oportunas y adecuadas a las agresiones recibidas.

TOPICO 4: PERSONAL			
RESP.	ENTREVISTADO UNO	ENTREVISTADO DOS	ENTREVISTADO TRES
UNO	El personal de oficiales tiene que estar capacitado en informática analistas operativos, el personal de suboficiales, en comunicaciones informática y en criptografía	Requisitos para el personal está relacionado con los distintos niveles de la organización: Ingenieros Militares en Informática, Ingenieros civiles en Informática conforman los cuadros superiores. Especialistas en Seguridad Información, en infraestructura y capacitadores.	El área RRHH constituye el centro de gravedad y factor determinante de la ciberdefensa [1], en carácter ideal el personal que esté afectado a dichas funciones debiera provenir de áreas tales como Informática, Comunicaciones, Inteligencia, Guerra Electrónica, Operaciones, Asuntos Jurídicos así como personas que hayan obtenido algún tipo de certificación internacional en el área de la seguridad de la información, hacking ético y la forensia informática.
DOS	se está tratando de generar una capacitación secundaria para el personal militar, para poder desempeñarse en este área. Luego, otras capacitaciones se darán según las necesidades	Referido a las políticas de personal civil se realiza una selección entrevistas personales presentación de la documentación que acredite sus conocimientos y aptitudes adquiridas. Una vez seleccionados pasan un período de prueba para confirmarlos posteriormente.	1En ciberdefensa, disponer de RRHH idóneos nos otorga la libertad de acción suficiente y necesaria para determinar (por propios medios, sin necesidad de asesoramiento externo) aspectos tales como la doctrina (organización y procedimientos) y los recursos tecnológicos que nos permitan alcanzar las aptitudes de ciberdefensa que hayan sido establecidas.
TÓPICO 5: INTERACCIÓN			
RESP.	ENTREVISTADO UNO	ENTREVISTADO DOS	ENTREVISTADO TRES
UNO	Tiene un alto grado de interoperabilidad con Fuerza Aérea y Ejército, efectuando intercambio de personal y capacitando, en la escuela técnica del ejército, que dicta cursos y especializaciones de distintos niveles.	referido al conocimiento de lo que están realizando las otras fuerzas, hasta el momento no se ha interactuado con las mismas a este nivel operativo. a partir de la creación y la puesta en ejecución del comando se presume que existirán fluidos contactos con las mismas.	Personal de la FAA interactuó con personal de las otras Fuerzas, durante las reuniones sostenidas para la redacción del Plan Estratégico de Ciberdefensa del EMCO.
DOS	dentro de lo que es la orgánica particular de ciberdefensa de la armada, se tiene contemplada la división Investigación y Desarrollo (I+D), donde se desempeñarían profesionales universitarios. Pero será en un paso futuro	Referido a la interacción con organismos civiles y organismos gubernamentales. Si se realizan. Al punto con universidades solo con la Universidad del Ejército.	En estas instancias iniciales aún no se han concretado.

Bibliografía:

Libros

Libicki, Martin C. Ciberdeterrence and Cyberwar. Rand Corporation. 2009.

Russel D Howard, Reid L Sawyer. "Terrorismo y Contraterrorismo"1º edición, Buenos Aires, Instituto de Publicaciones Navales.2005

Sten, Enrique. La Guerra Cibernética El Ciberespacio - La Cuarta Fuerza Editorial Dunken.

Manuales y Reglamentos

Argentina. Ministerio de Defensa. - MC-20-01 - 2013. "Manual de Estrategia y Planeamiento para la Acción Militar Conjunta, Nivel Operacional- La Campaña". Revisión. Buenos Aires. Estado Mayor Conjunto de las Fuerzas Armadas.

Argentina. Ministerio de Defensa RFD–99–01. Terminología Castrense de uso en el Ejército Argentino. CD - 01. Edición Año 2002.

Manual de Tallin- Sobre el derecho internacional aplicable a la guerra cibernética. Traducción oficial por el Ministerio de Defensa Argentino. Mayo 2014.

Documentos

Armada Argentina, Apuntes. Barrera, Marisa Eugenia "La formación y el perfil del cibersoldado"

Budapest University of Technology and Economics, Department of Telecommunications. "SKyWIper: A Complex Malware for Targeted Attacks". Equipo de análisis Skywiper. Budapest, año 2012.

ESGC, Escuela de Guerra Conjunta. "Lineamientos para la seguridad cibernética en un teatro de operaciones", Capitán de Corbeta Daniel Eduardo Giudice. Ciudad Autónoma de Buenos Aires, año 2013.

ESGC, Escuela de Guerra Conjunta. “Nuevas Tecnologías de Información y Comunicación (TIC) y su influencia en los teatros de operaciones (TO) modernos”, Eduardo Ignacio Llambí, Ciudad Autónoma de Buenos Aires, año 2011.

ESGN, Escuela de Guerra Naval. “Ataques Virtuales y la seguridad Informática”, Ciudad Autónoma de Buenos Aires. Capitán de Corbeta Rubén Héctor Silva, año 2013.

ESGN, Escuela de Guerra Naval. “La guerra de la información y sus efectos en la defensa nacional”, Ciudad Autónoma de Buenos Aires Capitán de Corbeta Alfredo Román Martin, año 2006.

ESGN, Escuela de Guerra Naval. La información como un objetivo vital “un estudio parcial de la guerra de la información”. Capitán de Corbeta Carlos Rubén Rivas. Ciudad Autónoma de Buenos Aires, año 2002

Escuela Politécnica de la Universidad Europea de Madrid “Ciber-terrorismo Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber-ataques terroristas” Ciudad de Madrid. Carlos Díez Molina, Javier Perojo Gascón, Juan José Penide Blanco, Mikel Arias R.Antigüedad, año 2011.

XV Workshop de investigadores en ciencias de la computación. “Inicio de la Línea de Investigación- Ingeniería de Software y Defensa Cibernética”, Paraná- Entre Ríos, Roberto Uzal, Jeroen Van de Graaf, Germán Montejano, Daniel Riesco, Pablo García

Universidad Nacional de San Luis, “La Universidad Nacional De San Luis En Netmundial”. Elaborado por Profesor Doctor Daniel Riesco.

Decretos

Decreto 889/2001. Modificación del Decreto Nº 20 de fecha 13.12.1999, en la parte correspondiente a la Subsecretaría de la Gestión Pública, dependiente de la Secretaría para la Modernización del Estado. Transformación del Instituto Nacional de la Administración Pública.

Revistas y Boletines

Colom Piella, Guillem.2006 "La revolución en los asuntos militares. Boletín de Información, España, número 295 noviembre 2006.

Flores Ana, "La Guerra en el Quinto Domino". Manual de Informaciones. Buenos Aires, número del volumen LIV, fascículo nº 4, octubre-diciembre 2012.

Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012.

GeeAlastair, "El oscuro arte de la ciberguerra" Manual de Informaciones, Campo de mayo, número de volumen LI, número de fascículo Nº2 abril-junio 2009.

Ortiz Javier Ulises. "La necesidad de un Nuevo Pensamiento Estratégico Frente A LA Guerra De La Información" La Revista. Buenos Aires, número especial. 2003

Poblete Jaime, ¿Revolución en asuntos militares o revolución en tecnológica militar? .Memorial del ejército de Chile. Edición nº 478 diciembre. 2006

Reppeto Guillermo. "La ciberguerra". Revista de la Escuela de Guerra Naval. Buenos Aires, número de volumen 51, diciembre 2001.

Torres Soriano Manuel. "Los límites de la Guerra de la Información". Ejército de Tierra español. Madrid, Número de volumen LXX, número de fascículo 818.junio 2009.

Páginas Web

Anónimo. "Canadá denuncia un ciberataque procedente de China". Diario El País. Recuperado de: *http://tecnologia.elpais.com/tecnologia/2011/02/17/actualidad/1297936863_850215.html*

Anónimo: "Cronología del 'caso Snowden', el joven que reveló el espionaje masivo de Estados Unidos" 20 minutos.es. Recuperado de: *http://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/*

Anónimo: "El Ejército de Brasil y Panda Security: juntos contra la ciberguerra" Infosertec. Recuperado de: *http://www.infosertec.com.ar/blog/?p=21483*

Anónimo. “guerra informática”. Recuperado de: http*://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica*

Anónimo “Internet de y para todos” Diario El país recuperado de: *http://elpais.com/elpais/2014/04/23/opinion/1398277986_745914.html*

Bejarano, José Caro. “El Control de Armas en la Era de la Información”. Instituto Español de Estudios Estratégicos Recuperado de: *http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI28a2012_InformationAge_ArmsControl_MJC.pdf. Mayo 2012.*

Brett T. Williams “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 2014*

Casar Corredera, José R. “Tecnologías y Servicios para la Sociedad de la Información”. Universidad Politécnica de Madrid. Enero 2005.

Castro, Luis “¿Qué es hacker?” recuperado de *http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es-Hacker.htm*

Cohen, Fred.“Influence Operations”. USA. Recuperado de: *http://all.net/journal/deception/CyberWar-InfluenceOperations.pdf. 2011.*

Cortes Pérez, Manuel. “El Ciberespacio. Nuevo Escenario de Confrontación”. Centro de Estudios del Ministerio de Defensa. España. Febrero 2012. Recuperado de: *http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf*

Cyberspace & Information Operations Study Center. Recuperado de: *http://www.au.af.mil/info-ops/cyberspace.htm#cyber. Mayo 2013.*

Dergarabedian, César. “La guerra cibernética “sale” de las computadoras y llega a la economía “real”. San Francisco. Recuperado de: http*://www.iprofesional.com/notas/156056-La-guerra-ciberntica-sale-de-las-computadoras-y-llega-a-la-economa-real”. Abril 2013.*

Federico Rosas, y Cecilia Ballesteros, Diario El País, “El futuro de internet se decide en Brasil”. Recuperado de:

http://internacional.elpais.com/internacional/2014/04/23/actualidad/1398219461_337462.html

Goetz John, Rosenbach Marcel and Szandar Alexander. "War of the Future: National Defense in Cyberspace". Recuperado de. *http://www.spiegel.de/international/germany/0,1518,606987,00.html. Febrero 2009.*

Lucas Nahuel Fudi. "La guerra cibernética en las fuerzas Armadas un desafío global" Recuperado de: *http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=1316:la-guerra-cibernetica-en-las-fuerzas-armadas-un-desafio-global-&catid=85:articulos&Itemid=107*

Ministerio de Defensa, "Argentina tendrá su propio centro de Ciberdefensa" Comunicado de prensa. Recuperado de: *http://www.prensa.argentina.ar/2014/05/14/49917-rossi-argentina-tendra-su-propio-centro-de-ciberdefensa.php*

Netmundial Multistakeholder Statement. Recuperado de: *http://netmundial.br/netmundial-multistakeholder-statement/*

Portal de la Armada Argentina recuperado de: *http://www.essa.ara.mil.ar/CarrerasEscalafones/NavalesIN.html*

Portal del Estado Mayor Conjunto de las Fuerzas Armadas, Ministerio de Defensa "Nuevas autoridades del Estado Mayor Conjunto de las Fuerzas Armadas" recuperado de: *http://www.fuerzas-armadas.mil.ar/2014-JUN-18-Nuevas-Autoridades-EMCOFFAA.aspx*

Portal de la Secretaría de Gabinete y Coordinación Administrativa. Jefatura de Gabinete de Ministros. Recuperado de: *http://www.jefatura.gob.ar/sgp/paginas.dhtml?pagina=27*

Ramírez, Gustavo. "Prepara EU ofensiva cibernética con 4 mil nuevos miembros en su Cibercomando". CiberPoliticos.com recuperado de: http*://ciberpoliticos.com/?q=EUofensivacibernetica4milCibercomando. Enero 2013.*

Rosa Jiménez Cano. "Nadie está a salvo de esta ciberguerra" Recuperado de: *http://elpais.com/diario/2010/12/10/sociedad/1291935601_850215.html*

Rozoff, Rick. “El Pentágono se asocia con la OTAN para crear un sistema de guerra ciberspacial global”. Recuperado de: *http://rebelion.org/noticia.php?id=114884 . 15 de octubre de 2010.*

Salanova, Antonio. “El sistema de mando y control conjunto en España”. Ministerio de Defensa. Recuperado de: *http://www.revista-ays.com/DocsNum10/PersAAPP/salanova.pdf. 2007.*

Stiennon, Richard. “Surviving Cyber War”. IT-Harvest. U.S.A. recuperado de: *http://www.slideshare.net. April 2009.*

The U.S. Cyber Consequences Unit. Recuperado de: *http://www.usccu.us/*