MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

TRABAJO FINAL INTEGRADOR

TEMA:

GUERRA CIBERNETICA

TÍTULO:

LINEAMIENTOS PARA LA SEGURIDAD CIBERNETICA EN UN TEATRO DE OPERACIONES

AUTOR: Capitán de Corbeta Daniel Eduardo GIUDICI

PROFESORA: Dra. Lucía Alejandra Destro

Año 2013

Resumen

Durante los últimos años la Guerra Cibernética o Ciberguerra se ha transformado en un desafío para aquellos que custodian la soberanía de los Estados.

Los que planifiquen acciones en un Teatro de Operaciones tendrán la preocupación de poder enfrentar un eventual y particular tipo de amenaza asimétrica, la guerra cibernética.

Si se considera que un ataque cibernético no reconoce límites y que sus perpetradores de manera anónima están en capacidad de afectar núcleos o instrumentos de importancia para el funcionamiento de un Estado, resulta pertinente el interés por el estudio y desarrollo de actividades que permitan a las Fuerzas Armadas estar preparadas para enfrentar este nuevo ambiente de guerra.

En la era cibernética, la creciente importancia de los sistemas de información en los ambientes de crisis y en los conflictos actuales revelan que la seguridad de las redes informáticas es crítica para la obtención de la victoria y el desarrollo de las actividades antes, durante y posterior al conflicto.

A partir de este trabajo se podrá comprender como el empleo efectivo de los medios y tecnologías cibernéticas facilitan y favorecen el dominio de las Fuerzas Armadas en un Teatro de Operaciones, en tanto éstas se sustenten en estructuras orgánicas con la adecuada distribución personal.

Contar con la capacidad para defenderse contra un ataque cibernético, debería ser un objetivo primordial para el Estado y una misión para las Fuerzas Armadas.

Es necesario contar con profesionales especializados y orientados al desarrollo de medidas de seguridad, tratamiento de la información, supervisión de la aplicación de medidas de seguridad cibernética y para adquirir tecnología y contratar servicios especializados con el respectivo análisis de riesgos ante un ataque cibernético.

El tratamiento de la información, su seguridad física y digital juntamente con el establecimiento de diferentes niveles de alarma, asegura el grado de preparación necesario para hacer frente a agresiones cibernéticas en el Teatro de Operaciones.

Palabras clave

Guerra Cibernética - Teatro de Operaciones – Defensa y Seguridad – Manejo de la Información.

Tabla de Contenidos

Introducción

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

Actores estatales y no estatales, con fuerte presencia en el desarrollo tecnológico como Estados Unidos, Japón o China, entre otros, o con pobres estructuras del poder nacional, pueden valerse de medios informáticos para atacar, corromper, infectar o desequilibrar plataformas e infraestructuras computarizadas del entorno mundial, regional o zonal, actuando de manera remota y anónima[1].

Durante el año 1988 se produjo el primer ataque cibernético a la "autopista de la información". Durante este año la internet fue afectada por un virus tipo "gusano" dando lugar al primer equipo de reacción rápida para enfrentar esta clase de contingencias y amenazas electrónicas.

Esta problemática fue creciendo hasta llegar a hacerse presente en el ámbito de las operaciones militares, como es el caso de las llevadas a cabo por fuerzas aliadas de la OTAN en Kosovo cuando hackers intentaron penetrar sistemas de información aliados, o también durante 1998 cuando estos obtuvieron acceso a las computadoras del Pentágono[2].

Con el apoyo de un estudio realizado por el Instituto Ponemon se demostró la generalización de los ataques cibernéticos y la predicción acerca de que una organización eventualmente será el blanco de un ataque de este tipo[3].

Es importante entonces detenerse en estos aspectos y optar por estar preparados a ser receptores de eventuales ataques cibernéticos que intenten desequilibrar las estructuras convencionales del Estado, sea en tiempo de paz o de guerra.

La creación de virus informáticos es sólo un ejemplo de cómo los estados, organizaciones o simplemente personas, pueden servirse de esto para "espiar" a otros. Por ejemplo el virus Flame fue desarrollado conjuntamente por Estados Unidos e Israel y creado para recoger información clave sobre las instalaciones nucleares iraníes, rastrear de forma secreta redes informáticas de Irán y controlar las computadoras de los funcionarios iraníes[4].

En 2010, Stuxnet y Flame afectaron instalaciones del plan atómico de Irán y además

1 Ponemon Institute LLC. (2010). First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies. Traverse City, Michigan: Ponemon Institute LLC. Baskerville, R. L., & Portougal, V. 2003. Pág. 20

2 Ponemon Institute LLC. "Possibility Theory Framework for Security Evaluation in National Infrastructure Protection. Journal of Database Management". Baskerville, R. L., & Portougal, V. A. Traverse City, Michigan, USA. 2003. Pág. 15

3 Ponemon Institute LLC. "2011 Cost of Data Breach Study: United States". Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC. Traverse City, Michigan, USA. 2012. Pág. 27

4 La información fue extraída de un artículo publicado por El mundo.es. "EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán". Disponible en http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html

exploraron la posibilidad de dejar sin comunicaciones a las fuerzas de seguridad y militares y realizar apagones masivos en los sistemas de energía y transporte conjuntamente con el bloqueo a las actividades comerciales en ese país[5].

Así, se podría llegar al extremo de que un país deje paralizada a una nación enemiga sin necesidad de una invasión militar y con sólo controlar su infraestructura electrónica como las redes de comunicación, usinas eléctricas y bancos[6].

Estas acciones, entendidas como objetivos de nivel estratégico están directamente ligadas con el desarrollo de las operaciones en el nivel operacional de la guerra en un Teatro de Operaciones.

Durante el 2010, Estados Unidos inauguró su Cibercomando el cual, de un modo general, tuvo como misión principal planear, coordinar, integrar, sincronizar y conducir actividades con el fin de dirigir operaciones y dar defensa a las redes de información que el Departamento de Defensa designe como vitales o de importancia dentro del poder nacional[7]. Esta iniciativa generó tanto en tecnología como en doctrina un efecto reflejo para otros países como Gran Bretaña, Corea del Norte, Corea del Sur y China, entre otros. Tal es así que éstos, bajo diferentes acepciones, han creado comandos que entienden en temas de guerra cibernética y buscan básicamente cumplir con los lineamientos que persigue Estados Unidos[8].

Se puede decir entonces, que la seguridad informática ha pasado a ser un área sensible para la defensa de un Estado, aumentando con el paso del tiempo la probabilidad de que agentes foráneos lleven a cabo actos de elevado nivel de hostilidad utilizando como alternativas, complejos y maliciosos programas que por su nivel de destrucción virtual reciben el nombre de armas cibernéticas[9].

Si bien en la actualidad existen formas de poder prepararse para enfrentar este tipo de contingencia, el Estado argentino se encuentra ante el problema de la falta de doctrina y adiestramiento necesarios para dar el correcto y preciso apoyo en un Teatro de Operaciones.

Con el advenimiento tecnológico y los avances en materia de información, los movimientos dentro del espectro cibernético y su llegada a los diferentes centros de gestión del Estado nacional argentino, hacen necesario cambiar el punto de vista y el paradigma sobre las políticas de seguridad y el concepto territorial sobre el que se custodia la soberanía.

---

5 Dergarabedian, César. “La guerra cibernética “sale” de las computadoras y llega a la economía “real”. San Francisco April 2013. Disponible en Iprofesional.com.

6 Tritz, Gerald L. “Cyberspace and the Operational Commander”. Naval War College. New Port. USA. 2010. Pag. 12.

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

8 Ramírez, Gustavo. “Prepara EU ofensiva cibernética con 4 mil nuevos miembros en su Cibercomando”. CiberPoliticos.com. Disponible en http://ciberpoliticos.com/?q=EUofensivacibernetica4milCibercomando. Fecha de captura 28 de enero de 2013.

9 Cyberspace & Information Operations Study Center. Disponible en http://www.au.af.mil/info-ops/cyberspace.htm#cyber. Fecha de captura, 01 de mayo de 2013.

En el Siglo XXI, los estados no pueden con exclusividad defender sus fronteras con medios militares. Actualmente, un ataque cibernético puede ocasionar el colapso de infraestructuras a gran escala, economía, servicios, redes, todas ellas fundamentales para el funcionamiento de la sociedad de una nación[10].

Las Fuerzas Armadas argentinas no se encuentran preparadas para hacer frente a este tipo de amenaza, que además extiende su agresión informática ilimitada en tiempo y espacio. Entonces, ¿cuáles serían las alternativas y lineamientos a seguir en el marco de la defensa nacional para desarrollar capacidades y recursos que permitan afrontar un ataque cibernético a los centros de comando y control en el Teatro de Operaciones argentino?

Para dar respuesta a este interrogante y dado el carácter tecnológico de la ciberguerra el objetivo principal de esta investigación es determinar las capacidades y lineamientos mencionados.

Asimismo y a los fines de contribuir al desarrollo del objetivo principal los objetivos específicos se enfocan en:

- Establecer áreas que estructuren la seguridad en el manejo de la información de la defensa en el Teatro de Operaciones a través de estructuras orgánicas que permitan la distribución del personal capacitado en el manejo de la información.
- Elaborar normas y medidas de seguridad física digital, para el tratamiento de la información en los centros de comando y control, determinando niveles de alarma para agresiones cibernéticas en el Teatro de Operaciones.
- Identificar en el mercado civil/militar, herramientas informáticas disponibles para el empleo defensivo contra agresiones cibernéticas, contemplando además la necesidad de formar oficiales especialistas en el área en cuestión.

Como hipótesis preliminar se sostiene que el desarrollo de estructuras orgánicas que aseguren el intercambio de datos, junto a la capacitación de personal en las áreas de empleo de redes y manejo de información dentro del ciberespacio permite asegurar la defensa de la infraestructura y medios militares argentinos en el Teatro de Operaciones.

Para llevar a cabo el presente trabajo se realizó una exploración bibliográfica y el análisis de diversas fuentes de información: artículos, trabajos de investigación e informes disponibles en Internet, regionales e internacionales, poniendo énfasis en los desarrollos llevados a cabo por las naciones vanguardistas en la temática. Además se consideraron las doctrinas de otros países y su grado de adaptación a la infraestructura de las Fuerzas Armadas de Argentina.

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 detallan las

10 Cohen, Fred. "Influence Operations". U.S.A. 2011. Pag. 10. Disponible en: http://all.net/journal/deception/CyberWar-InfluenceOperations.pdf.

áreas de una estructura orgánica para la seguridad cibernética en un Teatro de Operaciones. En el capítulo 2, se exponen normas y medidas de seguridad física digital, que actualmente Estados Unidos esta empleando, estableciendo además los niveles de alarma y seguridad necesarios para preservar las estructuras de comando y control en el Teatro de Operaciones. Finalmente, en el tercer capítulo se identifican en el mercado civil/militar, herramientas informáticas disponibles para el empleo defensivo contra agresiones cibernéticas, fundamentando, además, la necesidad de formar oficiales especialistas en su manejo.

1. Áreas y Estructuras Orgánicas para la Seguridad Cibernética en la Defensa de un Teatro de Operaciones

1.1 La amenaza: ciberguerra

Previamente al tratamiento de las áreas y estructuras orgánicas para la seguridad cibernética en un Teatro de Operaciones, se hace necesario visualizar algunas singularidades asociadas a la amenaza denominada ciberguerra.

El paradigma de la revolución tecnológica se instauró a lo largo de las últimas tres décadas y se focalizó en los avances principalmente vinculados a las áreas de las comunicaciones, manejo de la información y diseminación del conocimiento.

Los niveles de interconectividad, velocidad, simpleza y seguridad para que la información llegue a cualquier lugar del mundo, favorecieron las relaciones de la humanidad en todos los aspectos y sentidos.

Sin embargo, asociado a estos avances, también comenzaron a aparecer vulnerabilidades y falencias de los sistemas informáticos y de telecomunicaciones que no hacían otra cosa que buscar el colapso de las redes de información.

Durante el año 1988 se produjo el primer ataque cibernético a la "autopista de la información". Durante este año internet fue afectado por un virus tipo "gusano" dando lugar al primer equipo de reacción rápida para enfrentar esta clase de contingencias y amenazas electrónicas.

Tomando este evento y asociándolo con aquellos que lo llevaron a cabo, es donde aparecieron en escena y como parte integrante del ciberespacio, individuos que encontraron el tiempo y la oportunidad ideal para iniciar una serie de actividades delictivas. Estos individuos fueron denominados hackers.

En un principio buscaron popularidad a través de la demostración de sus capacidades para infiltrarse en las redes y sistemas de comunicación informáticos.

No pasó mucho tiempo hasta que un cambio en los intereses y motivaciones de estos individuos ampliaron el espectro de posibilidades de blancos y ataques. Terroristas, organizaciones criminales, extremistas políticos, movimientos fanáticos, servicios de inteligencia y fuerzas militares hoy hacen uso de los hackers o personal calificado para infiltrarse en las redes.

Si bien la comunidad internacional entiende como vulnerabilidades del ciberespacio al robo de identidad, fraude financiero y robo de información[11], actualmente la problemática ha alcanzado un nivel de inserción altísimo y con la aparición del ciberterrorismo y el ciberespionaje[12], los sistemas nacionales, civiles y de gobierno se ven afectados potencialmente por la capacidad que tienen estos de dañar seriamente las

11 Díaz Del Río Duran, Juan José. "La Ciberseguridad en el ámbito militar". Ministerio de Defensa de España. Diciembre 2010. Pág.118.
12 Ídem. Pág. 119.

infraestructuras críticas que lo componen.

A la hora de enfocarse en cuales son los elementos comunes y pasibles de ser blancos y que su afectación brinda un alto grado éxito de una operación de ciberataque, se puede generalizar que el mando, control, comunicaciones y redes de información son las más probables.

En los últimos años, hubo diferentes ciberataques a países por motivaciones políticas, como pueden ser los realizados contra Estonia, Georgia, Estados Unidos y Corea del Sur[13]. Esto da muestra la relevancia de la amenaza y, con el fin de no perder la carrera en esta temática, se hace necesario organizar una estructura orgánica y asignar áreas de injerencia para la atención del ciberespacio dentro del Teatro de Operaciones Argentino.

Actualmente, son varios los estados que comenzaron a realizar actividades orientadas a la obtención de la capacidad de empleo del ciberespacio. Eso permite pensar que en los futuros conflictos la ciberguerra puede convertirse en el primer escalón de la crisis y el ciberespacio, un ambiente de operaciones más junto con la tierra, el mar y el aire, pero con la salvedad que este los atraviesa a todos.

1.2 Capacidad necesaria

Los países en el marco regional de América del Sur, ya comenzaron los planeamientos y tareas orientadas a obtener capacidades que le permitan afrontar los desafíos impuestos por el ciberespacio y su segura navegación.

Sin embargo, la situación geopolítica y económica de la Argentina, hace que el desarrollo de lineamientos de estructuras orgánicas que aumenten el número de efectivos, al estado puede complicar el plan por las restricciones inherentes a las condiciones económicas y presupuestarias.

No obstante, la capacidad es necesaria y pese a lo anteriormente mencionado, resulta de utilidad diagramar un sistema que sustentado por la correcta estructura orgánica y la distribución de áreas de importancia en el manejo de la información, permita al instrumento militar y civil hacer frente a una amenaza cibernética dentro del Teatro de Operaciones argentino.

La necesidad de lograr completar una situación de alerta en asegurar la diseminación de la información conduce la necesidad de tomar medidas para conducir los sistemas de información de forma segura.

El ambiente de la información esta integrado por organizaciones y sistemas que se encargan de colectar, procesar, diseminar o actuar sobre la información. Como parte del ambiente de la información están los actores, que incluyen líderes, decisores, individuos y organizaciones.

El ambiente de la información es donde los seres humanos y los sistemas automáticos

13 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 219.

observan, orientan, deciden y actúan sobre la información y es este el principal ambiente de decisión. El ambiente de la información suma complejidad a la guerra moderna, que actualmente consiste en mar, aire, tierra y espacio (no geográfico), el ciberespacio. Sus dimensiones son la infraestructura, el almacenaje y el procesamiento de la información, tanto como la toma de decisiones.

1.3 Áreas del ciberespacio

Dentro del instrumento militar y pese a la eficiencia demostrada a los largo de la historia respecto al accionar militar conjunto, cada fuerza armada cuenta con áreas especificas para cada ambiente de guerra en donde es competente.

No siendo ajeno a este concepto central de la especificidad de cada fuerza, tierra, mar y aire ahora, con la necesidad de incorporar el ciberespacio, en el caso de conformarse un Teatro de Operaciones, los ambientes de guerra se dividirán en áreas a los fines de proporcionar una mayor eficacia y rapidez en las respuestas a las incidencias del enemigo.

Las información y su seguridad dentro del espectro de las operaciones militares, integra todos los aspectos de la información y su apoyo para intensificar el poder de combate, con el fin ulterior de cumplir con la misión y dominar el Teatro de Operaciones en tiempo y lugar necesarios, negando al enemigo su capacidad para la toma de decisiones[14].

Del estudio de la doctrina e información vigente en la Organización del Atlántico Norte (OTAN), específicamente desarrollada por España, se desprende que para el caso del ciberespacio y en materia de seguridad de la información pueden mencionarse cinco áreas[15]:

- Seguridad de la Información en las Personas
- Seguridad de la Información en los Documentos
- Seguridad de la Información en poder de las empresas
- Seguridad de la Información en las Instalaciones
- Seguridad de la Información en los Sistemas de Información y Telecomunicaciones

Cada una de estas áreas pese a agrupar una estructura particular, su accionar se centra en la adquisición, protección, administración, explotación y negación de la información[16].

El ciberespacio dentro del Teatro de Operaciones y respecto de la seguridad de la información, se nutre de dos grandes sectores: el militar y el global.

14 Anónimo. “Information Operations” Agosto 1996. Department of the Army. Pag. 2-3.
15 Díaz Del Río Duran, Juan José “La Ciberseguridad en el ámbito militar”. Ministerio de Defensa de España. Diciembre 2010. Pág. 238.
16 Anónimo. “Information Operations” Agosto 1996. Department of the Army. Pag. 2-3.

Dentro del militar se puede encontrar tres grandes grupos, el relacionado con las operaciones, el de la inteligencia y el de los sistemas de información, todos ellos interrelacionados, superpuestos y concurrentes.

En el caso del sector global de la información, involucra los sistemas de infraestructura nacional en general y las organizaciones internacionales (Cruz Roja, Organización Mundial de la Salud, etc.), la industria , la internet y los medios de comunicación masivos.

En función de ello y a los fines de posteriormente definir estructuras y responsabilidades, teniendo en cuenta el ámbito regional, la funcionalidad cooperativa de las naciones en la región de América del Sur, lugar donde de ser necesario y en función de la política se establecería un Teatro de Operaciones argentino, es conveniente agrupar y priorizar las áreas de manejo y seguridad de la información en:

- Seguridad de la Información en las Redes
- Seguridad de la Información para el Personal
- Seguridad de la Información en las Instalaciones
- Seguridad de la Información en las Telecomunicaciones

El área de seguridad de la información en las redes, se orientaría a llevar a cabo acciones dentro de las redes de los sistemas informáticos, buscando darle protección contra potenciales interrupciones, perturbaciones, inutilizaciones, degradaciones o engaños de los sistemas de mando y control, anulando la capacidad del enemigo de persistir en la acción ofensiva. Producto del alto nivel de inserción informático que se encuentra presente en todos los ámbitos, esta área engloba al resto, constituyéndose de manera transversal con respecto a las restantes.

En el caso del área seguridad de la información para el personal, se buscará por medio del establecimiento de protocolos, el monitoreo de las acciones llevadas a cabo por todos los usuarios de la red, estratificadas de acuerdo a los niveles de seguridad que cada personal por su función está autorizado. Además de otorgar al usuario de un perfil con derechos de acceso a la información, independientemente de donde fuera a conectarse a la red.

La seguridad de las instalaciones respecto de la información, debería poseer protocolos desarrollados para limitar y controlar a nivel técnico el uso de las instalaciones dentro del Teatro de Operaciones, evitando que material sensible se fugue o sustraiga sin autorización.

Finalmente y en materia de telecomunicaciones, es necesario establecer protocolos que limiten el empleo de internet y redes de trabajo.

1.4 Estructuras orgánicas de las áreas de Seguridad de la Información

Las estructuras orgánicas son fundamentales dentro de todas las organizaciones, sean estas civiles o militares.

Una sólida y bien diagramada estructura orgánica, permite conducir el desarrollo de las actividades, como así también canalizar los esfuerzos de la manera mas eficiente para lograr la correcta aplicación del poder militar.

En un Teatro de Operaciones en donde la preocupación es la ausencia de capacidad para contrarrestar un ataque cibernético y que presenta las vulnerabilidades respecto del manejo de la información, sensible para las fuerzas desplegadas en ejecución de un plan de campana, el sistema de información debe centrarse principalmente en maximizar las capacidades de comando y control en todos los ambientes, tierra, mar y aire.

Una estructura operacional hace a la base de los ambientes de guerra y esta debe estar enfocada en tres aspectos: el operacional, el sistemático y el técnico. Una vez que se cuenta con esta estructura, se comienza a crear un ambiente común de operación estandarizado e interactivo para la colección, almacenamiento y manejo de las bases de datos.

La estructura operacional establecerá la conectividad necesaria para la realización de los procesos, funciones, información y organizaciones. Deberá mostrar qué se hace, qué información se necesita, con que frecuencia y que grado de prioridad se le dará a la hora de tener que ejecutarse el intercambio de datos dentro del teatro.

El sistema estructural busca la identificación de relaciones entre los componentes del sistema de comando, control, información, comunicaciones, informática y crear una conectividad física dentro del mismo sistema de información. Emplea el contexto organizacional para mostrar el sistema de localización y estructuras de redes, ayudando a documentar las decisiones como es el caso de la selección de determinados anchos de banda y los protocolos de información.

La estructura técnica establece una serie de reglas de gobierno para ordenar, interactuar y necesita contemplar la interdependencia de todas las partes y elementos que de forma conjunta constituye el sistema de información. Especifica los estándares permisibles para designar las capacidades de comando control, informática, información y comunicaciones y resulta primordial para la creación y mantenimiento de los sistemas interactivos.

La integración con que cuenta el sistema de información, sea esta vertical u horizontal, facilita la agilidad táctica y operacional, la iniciativa, la profundidad, sincronización y versatilidad, todo esto que es nuclear para el éxito de las operaciones conjuntas.

La conectividad global es esencial para conectar la estrategia operacional con la táctica y la habilidad para programar y proyectar las operaciones en un Teatro de Operaciones.

Tanto en el ámbito militar como en el civil, los sistemas de información confiables cumplen con un rol importante dentro de esta estructura.

La aplicación de tecnologías de la información para digitalizar el Teatro de Operaciones se debe hacer a través de la integración de redes de comando y control que fluye transversalmente en cada nivel de la guerra.

La integración de esta red de comando y control con las unidades desplegadas en el teatro favorece la conectividad, la toma de decisiones y la habilidad para ejercer un control sobre el ritmo en como se llevan a cabo las operaciones y su nivel efectividad[17].

A continuación se enumeran algunas capacidades que mediante su adquisición y desarrollo pueden 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
- 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

1.5 Responsables orgánicos para áreas del ciberespacio

Hay países como es el caso de Estados Unidos, en donde la seguridad del ciberespacio se encuentra al nivel de manejo de la información del departamento de "Homeland Security", habiendo nombrado el actual gobierno del presidente Obama, un coordinador de ciberseguridad en la Casa Blanca, que es el responsable de supervisar la estrategia nacional para el ciberespacio[18].

Las dimensiones y estructuras creadas en Estados Unidos no son comparables a las del resto de los países. Luego de los ataques terroristas perpetrados en septiembre de 2001,

17 Salmerón, Rubén Benedicto. "Teorías y conceptos para entender formas actuales de hacer la guerra". Universidad Autónoma de Barcelona. Pág. 26.

18 Acosta Oscar Pastor, Pérez Rodríguez José Antonio, Arnáiz de la Torre, Taboso Ballesteros, Daniel Pedro."Seguridad Nacional y Ciberdefensa". Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones Ciudad Universitaria. Madrid. Octubre 2009. Pág. 55.

el Departamento de Estado impulsó estrategias de defensa territorial y desarrolló una amplia legislación relacionada con la ciberseguridad y la protección de infraestructuras críticas[19].

En Alemania, se ha formado la "Unidad de Reconocimiento Estratégico del Bundeswehr", compuesta por un grupo de diez profesionales, en su mayoría expertos en seguridad y, en el Reino Unido, se creó una oficina de ciberseguridad encargada de coordinar las capacidades defensivas y dar respuesta a intrusiones en redes[20].

En el ámbito nacional, España ha publicado la Política de Seguridad de la Información y sus normas de aplicación, tomando numerosas iniciativas para incrementar la seguridad de su información[21].

Como es lógico, también la Directiva de Planeamiento Militar estudia las capacidades relacionadas con el ciberespacio con las que las Fuerzas Armadas deben contar y el concepto de estrategia militar, describe el nuevo escenario estratégico en el que la ciberseguridad es tenida en cuenta y se analizan las tendencias y previsiones en este campo[22].

Por este motivo, muchos ejércitos están desarrollando capacidades ofensivas y defensivas en el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades[23].

En el nivel regional, la República Federativa del Brasil ha impulsado programas de desarrollo tecnológico y establecido pautas para la atención de la seguridad cibernética. Todo ello apoyado por la consiguiente asignación presupuestaria para afrontar los desafíos financieros.

El análisis necesario para identificar a un atacante puede llevar meses e incluso puede suceder que no se tengan medios para responder. Además, los ciberataques normalmente se originan en servidores situados en países neutrales y las respuestas pueden tener consecuencias imprevistas a sus intereses, razón además por el que el uso de este tipo de reacciones debe estar siempre bajo un mando estratégico que tenga una visión integral y global de la situación[24].

En este sentido y dada la complejidad del ambiente cibernético y su alcance es necesario establecer autoridades de acreditación. En el ámbito de la seguridad de la información se entiende por acreditación a la autorización otorgada a un sistema por la autoridad de acreditación, para manejar información clasificada hasta un grado estipulado y

19 Ídem. Pág. 29.

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

21Anónimo. "Seguridad de la Información". Ministerio de Defensa de España. Disponible en: http://www.defensa.gob.es/politica/infraestructura/seguridad-informacion/.

22 Ídem.

23 Anónimo. "Pentágono advierte que los ataques cibernéticos son 'actos de guerra'". Londres. Junio 2011. Disponible en: http://www.seguridad.unam.mx/noticias/?noti=4646

24 Ferrero, Julio Alberto. "La ciberguerra, génesis y evolución". Revista General de Marina. España. Enero-Febrero 2013. Pág. 82.

de acuerdo a unas determinadas condiciones de integridad o disponibilidad y de acuerdo al concepto de la operación[25].

Esta acreditación siempre deberá estar basada en cuales son los requisitos específicos de seguridad del sistema y en los procedimientos operativos de seguridad específicos, aparte de ser necesario un análisis de riesgos y un concepto de operación para la obtención de la citada autorización[26].

En el caso de asignar responsabilidades para la administración, ejecución y control de las tareas en el ciberespacio, entre las que se encontrarán además las mencionadas autoridades de acreditación, se mencionan a continuación algunas propuestas, sin explicitar el detalle de su operativa en particular:

- Ministro de Defensa como autoridad máxima de acreditación de la seguridad de los Sistemas de manejo de la información
- Ministro de Planificación Federal, Inversión Pública y Servicios, como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones.
- El Jefe de Estado Mayor Conjunto, tiene a cargo el control y acreditación de los sistemas conjuntos de Comando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica.
- Director Nacional de Inteligencia Estratégica Militar, como administrador y controlador de los organismos que tengan a su cargo sistemas o redes para el intercambio de información sensible
- El Jefe de Estado Mayor del Ejército, la Armada y la Fuerza Aérea, en los Sistemas específicos de sus respectivas fuerzas.

2. Normas, Medidas de Seguridad y Niveles de Alarma para el ciberespacio

2.1 Normas y Medidas de Seguridad

La cantidad de amenazas presentes en el ciberespacio es abundante, pero a los fines de diferenciarla se puede dividir en la calidad y grado del daño y el grado en cuanto a nivel de abstracción de la organización atacante.

La estrategia de Seguridad Nacional de los Estados Unidos para el Ciberespacio de febrero 2003 reconoce que la seguridad en el manejo de la información debe ser un esfuerzo coordinado entre los gobiernos de los estados, el sector privado y los ciudadanos[27].

Esto es importante puesto que a través de la concientización de la sociedad, respecto

25 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 238.
26 Ídem. Pág. 239.
27Avalos, Marco Carlos. "Ciberespacio y Cibercultura". Pág. 6. Disponible en: gabrieldjs.wikispaces.com/file/view/Ciberespacio+y+cibercultura-1.doc.

del grado de amenaza potencial a la que se encuentran expuestos los sistemas informáticos en general, permite preparase y tomar medidas de acuerdo al alcance e importancia de su organización y entorno, coadyuvando a la seguridad nacional.

La estrategia para el ciberespacio desarrollada por Estados Unidos consta de cinco líneas estratégicas, con la correspondiente asignación de responsabilidades y acciones que estas deben perseguir para alcanzar los objetivos o cumplir con sus misiones.

Estos lineamientos estratégicos son[28]:

- **Sistema de respuesta nacional de seguridad en el ciberespacio**. Para ello propone diversas acciones, entre las que destacan, la mejora de la gestión de incidentes, ampliar el sistema de alerta ante ciberataques, realizar ejercicios de coordinación o mejorar el intercambio de información público-privado.
- **Programa de reducción de amenazas y vulnerabilidades**. Para ello propone diversas acciones, entre las que destacan, la mejora de las capacidades de las fuerzas de seguridad (FBI y otras agencias policiales, la mejora del control de los sistemas SCADA o profundizar en el conocimiento sobre amenazas y vulnerabilidades.
- **Formación y concienciación en el ciberespacio**. Este programa estaba preparado para cinco tipos de audiencias; ciudadanos y pequeñas empresas, empresas consideradas estratégicas (especialmente las que gestionan infraestructuras críticas), universidades y centros de investigación (especialmente los que dispongan de gran capacidad de cálculo), sector privado (especialmente el que disponga de sistemas SCADA) y gobiernos locales y estatales.
- **Asegurar el ciberespacio gubernamental**. Las acciones a realizar en el gobierno federal fueron el seguimiento de la evolución de las amenazas y vulnerabilidades y la implementación de las mejoras de seguridad adaptadas a estas, el impulso de la alianza nacional para asegurar la información (NIAP), la mejora de la seguridad de las redes sin cables, la mejora de los requisitos de seguridad en la subcontratación y en las adquisiciones y la mejora en la realización de los procesos de auditoría o inspección. Además se debe impulsar la seguridad en los gobiernos locales y estatales.
- **Cooperación nacional e internacional.** Como líneas de actuación destacan el refuerzo de las actividades de contrainteligencia, la mejora de las capacidades de prevención y atribución de un ataque y la coordinación entre las diferentes agencias. Internacionalmente se intentará mejorar los canales de comunicación y que se adopten en las legislaciones nacionales los acuerdos sobre cibercrimen.

28 Anónimo. “International Strategy for Cyberspace”. Casa Blanca. Estados Unidos. Mayo 2011.

Para el desarrollo de esta estrategia, se impulsa el US-CERT que proporciona apoyo en la respuesta ante ciberataques contra la parte civil del gobierno nacional y tendrá la responsabilidad de relacionarse con los gobiernos locales, estatales y la industria[29].

En el ámbito del Ministerio de Defensa existen muchas iniciativas asi también como en el caso de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas como la Agencia de Seguridad Nacional. Esta agencia tiene un departamento encargado del aseguramiento de la información que se focaliza en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de cifra y gestión de claves de los mismos y en la formación y concienciación de seguridad[30].

Las redes de Comando y Control que manejan información clasificada poseen un alto nivel de protección y no están conectadas a Internet. Sin embargo, esto no garantiza su seguridad. Todos los sistemas operativos y gran número de aplicaciones empleadas en redes clasificadas son adquiridos en el ámbito comercial y por ello requieren una actualización continua, lo que se realiza a través de Internet en servidores separados, siendo ese el punto vulnerable de intrusión[31].

Además, se debe tener en consideración que desde el punto de vista del hardware la mayoría de los componentes electrónicos son de manufactura no nacional y éstos pueden incluir en su «firmware» un código dañino no detectable o de muy difícil detección que se active en un momento determinado a raíz de un comando seleccionado, produciendo el colapso del sistema o equipo[32].

La era de la información ha alterado la distribución de poder, aumentando la complejidad de los sistemas de información y restando importancia a las distancias geográficas, reduciendo los tiempos de reacción[33].

La Organización del Atlántico Norte, se ha encargado de diseñar una red que le permite mantenerse actualizada respecto de los estos cambios.

Para que el Comandante de un Teatro de Operaciones pueda decidir y esta decisión sea la correcta y adecuada para la conducción de las operaciones, la información tiene que ser precisa, íntegra, y oportuna. Para ello es necesario una capacidad que integre todos los componentes del medio operativo, sensores, elementos de decisión y plataformas de armas, desde el nivel político-estratégico hasta el nivel táctico, a través de una infraestructura de

29 Anónimo. Department of Homeland Security. Disponible en: http://www.us-cert.gov.
30 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 277.
31 Salanova, Antonio. "El sistema de mando y control conjunto en España". Ministerio de Defensa. 2007. Disponible en: http://www.revista-ays.com/DocsNum10/PersAAPP/salanova.pdf.
32 Ferrero Albert, Julio. "La Ciberguerra. Génesis y Evolución". Revista General de Marina. España. Enero – Febrero 2013. Pág. 87.
33 Bejarano, José Caro. "El Control de Armas en la Era de la Información". Instituto Español de Estudios Estratégicos. Pág. 2. Nro. 28. Mayo 2012. Disponible en: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI28-2012_InformationAge_ArmsControl_MJC.pdf.

información y redes[34].

Para poder lograr este nivel de eficiencia y normas de seguridad las fuerzas desplegadas en el Teatro de Operaciones deben cumplir con los siguientes principios[35]:

- Las fuerzas deben estar interconectadas a fin de mejorar el intercambio de información, la percepción de la situación, permitiendo la colaboración, sincronización y mejora de la velocidad en la toma de decisiones.
- Todo usuario tendrá un perfil de derechos de acceso a la información, dondequiera que se conecte a las redes de telecomunicaciones.
- Es vital la total interconexión con otros sistemas, incluso con ONG's.
- Todos los usuarios precisarán recibir la formación y adiestramiento adecuados para utilizar adecuadamente cada uno de los sistemas que integran la red de la defensa.
- Necesitarán emplear todas las herramientas disponibles del sistema para extraer la información.
- Procesos de adquisición más flexibles y la búsqueda de socios adecuados en la industria.
- Consideración de alianzas ya que habrá algunos estados y organizaciones que no estarán dispuestos a compartir cierta información sensible.
- Habrá que tener previsto el poder continuar las actividades en modo degradado y evitar el colapso de la red, contando con medios alternativos de comunicación para mantener activos los elementos clave de la red de redes.

Emulando estos principios establecidos por la doctrina de los Estados Unidos y desarrollando una infraestructura de clave pública como apoyo a la seguridad para el acceso a las redes y a los sistemas de información, junto al cifrado y el empleo masivo de la firma electrónica y el uso de chips en las tarjetas de identificación personal, se concretarían en el ámbito de la defensa argentina, normas de seguridad básicas que darían la base para continuar con el desarrollo avanzado de otras técnicas y procedimientos que permitan preservar y dar seguridad al procesamiento de la información.

2.2 Niveles de Alarma

Los niveles de alarma buscan alertar al sistema, personal y redes dentro del Teatro de Operaciones para que obre en consecuencia y asigne prioridades para atender las diferentes contingencias que atenten contra la seguridad de la información en las distintas áreas y sistemas que conforman el ciberespacio.

34 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 228.
35 Ídem. Pág. 229 – 230.

Estados Unidos continúa asignando el nivel de defensa, relacionándolo con las acciones a ser tenidas en cuenta en el caso de ser establecido.

Respecto del ciberespacio cuenta con cinco niveles de defensa[36]:

- DEFCON 1, advertencias para viajes. El gobierno advierte sobre la protección de la información cuando se viaja a otros países.
- DEFCON 2, los estados investigan las redes en busca de vulnerabilidades.
- DEFCON 3, amplio robo de información con la intención de adueñarse de información secreta perteneciente a la industria, fuerzas militares y situación geopolítica.
- DEFCON 4, ataques dirigidos a instalaciones militares o gubernamentales. Perdida de información critica y daño colateral.
- DEFCON 5, ataque entre estados maliciosos con la intención de destruir la infraestructura de comunicaciones y desactivar el proceso de los negocios incluyendo los procesos financieros.

En principio resultaría conveniente la asimilación de estos niveles de alarma dentro del Teatro de Operaciones argentino, prestando atención a los posibles cambios que pudieran surgir producto de las prácticas y adiestramientos que se lleven a cabo para ajustes del sistema integral de seguridad cibernética.

3. Herramientas y formación de especialistas para el ambiente cibernético

3.1 Tipos de Amenazas

Dentro del ciberespacio, existe un amplio espectro de amenazas que pueden ser del tipo: malware, spyware, gusanos, troyanos, virus, intrusiones a las redes de información y operaciones, evolucionando y desarrollándose nuevos tipos con los avances tecnológicos. Cada una posee un nivel de impacto y agresión relacionado directamente con el rol y las funciones del objetivo o blanco a atacar, debiéndose tener en cuenta a la hora de seleccionar el sistema defensivo a emplear.

Durante el 2008, se comprobó que un virus introducido por medio de un dispositivo de memoria flash, ocasionó la falla técnica de la computadora de vuelo del Spanair 5022, originando que este se precipitara a tierra[37].

Asimismo y en función del objetivo buscado, las amenazas pueden hacerse efectivas por medio de:[38]

36 Stiennon, Richard. "Surviving Cyber War". IT-Harvest. U.S.A. April 2009. Disponible en: http://www.slideshare.net.

37 Srimoolanathan, Balaji."Cyber Security – From Luxury to Necessity". Febrero 2011. Pág. 3.

38 Anónimo. "Guía/Norma de Seguridad de las TIC (CCN-STIC-400)". Centro Criptológico Nacional. España. Mayo 2013. Pág. 107.

- Botnets, conjunto de computadoras ejecutando programas maliciosos sincronizadas bajo una infraestructura de comando y control.
- Denial of Service, ataque a una red de computadoras por medio de una inyección en el servidor de falsas solicitudes de permisos y que se busca interferir el normal tráfico de datos e información.
- Hacking, consiste en el intento de una persona, no autorizada y con propósitos nocivos, de acceder al sistema de información, sin importar si este intento es eficiente o no
- Key Stroke Logging, método empleado para interceptar la información de cada tecla presionada por un usuario en un sistema de teclado, que busca el robo de claves o información. Este puede ser un dispositivo o un programa.
- Malware, este es un término genérico que concentra diferentes tipos de programas, diseñados para atacar, degradar o prevenir el uso de las telecomunicaciones.
- Phishing, una forma de fraude a través del internet en donde se busca el robo de información sensible por medio del engaño al usuario.
- External Access, es el simple método de acceso por medios físicos a una red de información.

El cifrado o encriptación de la información es un aspecto imprescindible a tener en cuenta en la era de la información, en donde a nivel global las tecnologías y su avance hacen necesario el desarrollo de estos equipos y/o técnicas acordes a las exigencias de los usuarios.

Por ello es vital poder desarrollar algoritmos y procesos de fabricación de equipos criptográficos nacionales pues esta es la única manera de poder tener un nivel de seguridad verificable durante el intercambio de información.

Existen desarrollos de diferentes equipos para el cifrado de la información. Sin embargo, dentro de sus características fundamentales deben brindar capacidad de interoperar con cifradores que tengan diferentes redes acceso, interoperabilidad en el nivel nacional y con aliados, módulos reprogramables y certificación múltiple[39].

Esta capacidad de desarrollo de tecnología y software, conjuntamente con la fabricación de insumos electrónicos asociados al área informática, deberían ser un monopolio del Estado por el grado de sensibilidad del ambiente cibernético y por ser la manera de brindar eficiencia y seguridad al sistema de defensa, sin dejar de lado la potenciación y posicionamiento en el ámbito regional que se adquiriría como país respecto del factor de poder científico-tecnológico.

39 Srimoolanathan, Balaji."Cyber Security – From Luxury to Necessity". Febrero 2011. Pág. 4.

3.2 Acciones Defensivas

Luego de haber definido los tipos de amenazas, es importante establecer, sobre todo por el carácter asimétrico que posee la guerra cibernética, cuales serian tentativamente las acciones que podrían esperarse y para las que se tuviera que estar preparado en un Teatro de Operaciones.

Independientemente del tipo de amenaza cibernética, las acciones que se pueden llevar a cabo dentro de dicho teatro sin importar donde se encuentre ubicado, pueden ser defensivas u ofensivas.

Sin embargo, y de acuerdo al marco legal vigente para el instrumento militar argentino, la ausencia de hipótesis de conflicto y el nivel de seguridad cooperativa alcanzado en la región, se pondrá atención en las acciones defensivas, ensayando una suerte de ordenamiento por fases:

- Alistarse para un ataque a los sistemas y a las redes de la información.
- Replicar el ataque.
- Recobrar las capacidades operativas de los sistemas y de las redes de información.

¿Pero en que consiste la preparación para establecer y asegurar la red cuando se habla de seguridad de la información?

En el análisis de los modos de operación y de la forma de canalizar la problemática por parte de otros estados, se pudo observar que generalmente es necesario recurrir a las bases de poseer una arquitectura de defensa en profundidad, mecanismos que garanticen el flujo de información, y un comando y control sólido y eficiente. Por otra parte, es necesario que las herramientas encargadas de obtener la información a ser procesada por estos sistemas y redes y por los sensores, externos e internos a la red, estén en capacidad de detectar, erradicar y bloquear las amenazas.

Cuando se dice replicar un ataque, se traduce en la implementación de conceptos relacionados con los controles de configuración dinámica, direcciones IP para tiempos de crisis y conflicto, saltos de frecuencia, método ya utilizado en las comunicaciones de radiotelefonía, intercambio físico y virtual de equipos en medio de la operación, técnicas de engaño, trampas de red y el uso de nombres para servidores que con intención buscan ser engañosos[40].

No obstante, es necesario que el personal avocado 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 pudieran perder los enlaces y nodos y, redireccionar los ataques proyectados por el enemigo hacia

40 Franz, Timothy. “El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación”. Air & Space Power Journal en Español. 2012. Pág. 50.

rutas sin salida.

Es vital por otra parte poder detectar en donde la red apoya a la misión, decidir cuándo y dónde se puede soportar una perturbación al sistema, ya que no necesariamente todos los ataques pueden ocasionar la pérdida o degradación de la red, haciendo que la misión deje de ser aceptable. Es positivo como decía Sun Tzu, hacer creer al adversario que su ataque está obteniendo el efecto o éxito esperado arrastrándolo a continuar invirtiendo recursos y tiempo en un objetivo desechable, permitiendo atender otras prioridades[41].

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. La seguridad de la información debe tener dos ámbitos de muy diferentes objetivos y características: la de comando y control y la de propósito general[42].

Para ello es necesario establecer una plataforma informática y arquitectura técnica que se oriente hacia un escenario cuya principal característica sea la existencia de dos únicas redes de área extensa para dar soporte a todos los sistemas de información del Teatro de Operaciones[43].

Una de las redes para Comando y Control Militar, cuyo despliegue y extensión se correspondería con el de los Puestos de Comando y los Centros de Comunicación. Esta debería interconectarse con los entornos tácticos y con las redes de sensores que fuera necesario. Desde el punto de vista de la seguridad, al ser su orientación de carácter eminentemente clasificado y de utilización para operaciones y planeamiento militar, los sistemas que la componen necesitarían estar acreditados en un nivel de clasificación adecuado, normalmente reservado y confidencial, estableciendo medidas de seguridad y cifrado[44].

La otra red de tipo Corporativa de Propósito General que daría soporte a todos los sistemas de información que no fueran específicos para mando y control y que se extendería a todos los emplazamientos. Este entorno incluiría la conexión a Internet del Ministerio de Defensa a través de un punto de acceso común para todos los usuarios y que la red de Propósito General tendría con el exterior[45].

Respecto de las Redes de Área Local con carácter general, los emplazamientos en el Estado Mayor Conjunto deben disponer de una LAN integrada en la WAN de Propósito General. Además, en aquellos emplazamientos que lo requieren, se deberían establecer LANs para Mando y Control, físicamente aislada de la anterior e integrada en su

41 Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012. Pág. 49 – 50.
42 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 244.
43 Villarroya Quintero, José Luis. "Las TIC en el Ministerio de Defensa". Ministerio de Defensa. España. Junio 2012. Pág. 140.
44. Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 244.
45 Ídem.

correspondiente WAN. Por último, en aquellos emplazamientos que incluyen un Centro de Procesamiento de Información Inteligencia debería existir una tercera LAN conectada también a la WAN para Comando y Control[46].

Como se pudo ver existe una variedad de maneras de conectarse a la red y transferir información de manera segura. Sin embargo, no se debe dejar de lado para maximizar estas medidas contar con sistemas de reconocimiento de retina, huellas digitales, reconocimiento de cara, firma electrónica, acceso al sistema por medio de identificación y microchip, que son algunas de las ofertas que se encuentran habilitadas en el mercado para hacer frente a los desafíos impuestos por la seguridad en el ciberespacio[47].

Finalmente y sin querer cerrar la gama de posibilidades que pudieran presentarse dentro de este punto, es necesario que la respuesta defensiva efectiva conlleve la aptitud para saber combatir integralmente y descentralizadamente dentro de la red de comando y control.

3.3 Formación y Adiestramiento de Especialistas

Es esencial, a la hora de buscar la adquisición de nuevas capacidades para cualquier ámbito ya sea este civil o militar, asentarse en la formación del personal porque esto constituye el pilar para la gestión eficiente de una organización.

En el ámbito de la defensa en general y en el del ambiente del ciberespacio en particular, la ciberguerra se caracteriza por su amplio espectro de injerencias y requiere por parte del personal, que este posea una especialización detallada y especifica ya que, dentro del ciberespacio y la tecnología cibernética, se pueden encontrar diversos campos de especialización.

Comandos de guerra cibernética ya establecidos como es en el caso de Estados Unidos, se encuentran trabajando para formar equipos de trabajo orientados por tareas específicas, apuntadas a acompañar las tácticas, técnicas y procedimientos doctrinarios relacionados con la ciberguerra[48].

Debido a la dificultad para encontrar personal capacitado en el área cibernética, se complica la constitución de estos equipos de trabajo, siendo así que el comando de guerra cibernética optó por enfocarse en el cumplimiento de tres misiones: defender las redes de información; apoyar a los comandantes en el Teatro de Operaciones; defensa contra un ataque cibernético[49].

Resulta esencial efectuar la apertura a la convocatoria para formar ciberguerreros desde el mismo inicio de su carrera de formación, debiendo poseer las aptitudes

46 Anónimo. “Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio”. Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 244.
47Cohen,Fred. “Influence Operations”. USA. 2011. Disponible en: http://all.net/journal/deception/CyberWar-InfluenceOperations.pdf. Pág. 10.
48 Wasserbly, Daniel. “Cybercom formulating offensive teams”. Jane’s Defence Weekly. Washington. 2013.
49 Ídem.

psicofísicas, nivel intelectual y vocación militar acorde a las exigencias propias de las operaciones en el ambiente del ciberespacio.

Los profesionales dedicados a desenvolverse en un ambiente de ciberguerra deben contar un complejo conjunto de habilidades, que les permita establecer, monitorear y proyectar el poder de combate en el ciberespacio.

Cada uno de este personal calificado debe contar con un conjunto de responsabilidades y habilidades, que en función de la tarea asignada cumpla con operaciones de carácter defensivo y ofensivo.

Asimismo, y a los fines de poder desarrollar tanto operaciones ofensivas como defensivas, también es necesario un cuerpo técnico que será el encargado de apoyar el sistema de guerra cibernética y la infraestructura, interviniendo en la instalación, configuración y mantenimiento de los componentes de cada equipo, computadoras, enrutadores, conmutadores y programas de software[50].

Como una consecuencia de lo anterior se desprende que los profesionales dedicados al ambiente de guerra cibernética deben ser entendidos en el desarrollo y programación de software. De esta manera se lograría cubrir el espectro completo de tareas que pudieran presentarse en un Teatro de Operaciones tales como son: la preparación, la ejecución y la supervisión de las acciones.

Si bien existe una distinción entre las operaciones ofensivas y defensivas, en lo que respecta a los cibersoldados y cuando se habla de operaciones ofensivas, estos deberían calificarse y conocer las capacidades tecnológicas del adversario como así también las funciones de sus redes de información y además contar con conocimientos para la operación de herramientas informáticas capaces de infiltrar virus o amenazas en las redes enemigas. En el caso de las operaciones defensivas, estos profesionales tendrían que poseer capacidades aptas para controlar las diferentes áreas del ciberespacio (propuestas en el primer capítulo de este trabajo) y que pueden variar desde una simple red de área local dentro instalaciones o plataformas de comando y control, hasta el caso de ejercer el control de una red global.

Para ello, los defensores del espectro cibernético necesitan poseer un conocimiento cabal de las tecnologías que inciden y que pueden emplearse para su accionar, teniendo en cuenta la importancia que posee la salvaguarda de la información.

A estos profesionales se los puede agrupar dentro de cuatro funciones diferentes, a saber. 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

50 Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012. Pág. 43 – 44.

y finalmente, desarrolladores de ciberguerra, que diseñan y crean herramientas y armas para la ciberguerra[51].

Actualmente, producto del avance tecnológico y de la creciente presencia de esta amenaza, se puede observar una inclinación por parte de las generaciones más jóvenes a introducirse en el sector de Tecnologías de la Información. Aquí es donde un programa de incorporación, tanto a nivel de los institutos militares como por medio de programas de asimilación para personal civil especializado en este sector, haría posible solucionar las contingencias que se pueden presentar en un Teatro de Operaciones.

Sin embargo, estudios llevados a cabo por el Instituto SANS demuestran en el caso del Reino Unido, la creciente necesidad que actualmente presenta la infraestructura estatal en lo que respecta a la formación de profesionales de seguridad, tanto militares como civiles[52].

Las Fuerzas Armadas españolas, pese a la problemática que trae depender de agentes externos al ambiente de la defensa respecto de las actividades llevadas a cabo en el ámbito de la seguridad nacional, actualmente apoyan sus necesidades de dar seguridad a la información en las empresas de servicios informáticos. Estas son una solución de compromiso inmediata y eficiente, sobre todo teniendo en cuenta el elevado costo monetario en el medio de una crisis económica, que ralentiza e incluso impide el desarrollo de actividades orientadas a solventar las previsiones y necesidades diversas de los programas de seguridad de la información[53].

Conferencias, simposios, seminarios, cursos online, cursos en los programas de formación específicos para cada fuerza y conjuntos, además del estímulo por parte del Ministerio de Defensa argentino a que su personal y el de cada fuerza armada se capacite en universidades por medio de la realización de cursos de posgrados, pueden presentarse como iniciativas accesibles y formadoras.

Asimismo, y con el objeto de concientizar y sensibilizar al ámbito-cívico militar, el Ministerio de Defensa en coordinación con el Ministerio de Planificación, Desarrollo e Infraestructura y el Estado Mayor Conjunto de las Fuerzas Armadas, debería instrumentar jornadas anuales orientadas a la seguridad de la información.

Es el caso de países como España donde cada año se llevan a cabo jornadas en el CESEDEN, denominadas Jornadas de Seguridad de la Información del MINISDEF (Ministerio de Defensa de España) y que en su última edición contaron con la asistencia de 350 participantes[54].

El ciberespacio abarca muchas tecnologías configuradas dentro de redes que realizan una amplia gama de funciones. Aunque no existe una definición de ciberespacio

51 Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012. Pág. 43 – 44.
52 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 247.
53 Ídem. Pág. 253.
54 Ídem. Pág. 23.

aceptada universalmente, la mayoría de expertos concuerda en que tiene gran alcance e incluye una multitud de sistemas conectados en red que varían desde las redes administrativas más comunes, por ejemplo una LAN de una casa u oficina, pasando por comunicaciones de larga distancia basadas en el espacio, hasta complejos sistemas de control para activos de infraestructura vitales[55].

Para defender de forma efectiva una red, el equipo de ciberguerra debe entender las tecnologías que comprenden la red y la función que ésta realiza (es decir, la misión que apoya).

Las amenazas han trascendido los ataques contra redes administrativas comunes y sitios web para demostrar efectos contra recursos de infraestructura críticos como control de tráfico aéreo, pozos petroleros, servicio de telecomunicaciones y sistemas de control y adquisición de datos para administración de servicios públicos.

Los objetivos militares comunes representan una variedad de funciones construidas con una mezcla de tecnologías disponibles comercialmente, y tecnologías propias que van más allá de nuestra experiencia ofensiva actual. Para ambas, se puede asumir razonablemente que con el tiempo el nivel de sofisticación de la amenaza aumentará[56].

Aunque todos necesitan conocer los fundamentos de su dominio, cada uno debe especializarse en plataformas, misiones y áreas del ciberespacio específicas. De lo contrario, la magnitud de conocimiento requerido para que cada individuo entienda cómo afectar ofensivamente o proteger defensivamente todas las funciones y tecnologías dentro del ciberespacio tardarían más que toda una vida de aprendizaje[57].

Los profesionales de ciberguerra actuales vienen de los campos profesionales de comunicaciones e información. Como tales, se han concentrado históricamente en mantener las comunicaciones en funcionamiento y no en comprender completamente las misiones apoyadas por cada enlace o nodo de comunicaciones. En consecuencia, el verdadero entendimiento del impacto de la misión que causa la pérdida de un enlace o nodo ocurre comúnmente sólo después que la pérdida tiene lugar y los clientes comienzan a quejarse.[58]

Por medio del uso de las tecnologías de la información, se hacen posible casi todas las actividades tales como: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real. Todas estas funciones dependen de sus redes de comunicaciones e informáticas que, en el caso de EEUU por ejemplo, consisten en más de 15.000 redes y siete millones de terminales informáticos distribuidos en cientos de

55 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 247 – 248.
56 Franz, Timothy. "El Profesional de la Ciberguerra, Principios para Desarrollar la Próxima Generación". Air & Space Power Journal en Español. 2012. Pág 50 -52.
57 Ídem. Pág. 45.
58 Ídem. Pág. 49.

instalaciones en docenas de países, para cuyo funcionamiento mantienen más de 90.000 especialistas[59].

La formación del personal, vaya a ser 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, deberán pasar por un proceso de selección y poseer como mínimo las siguientes acreditaciones que a continuación se recomiendan:

Oficiales Superiores, Jefes y Subalternos:

- 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.

Personal de Suboficiales:

- Formación académica en el grado de Técnico Electrónico o Informático.
- Formación en administración y mantenimiento de redes informáticas.

Los ciberguerreros deben adquirir conocimientos y pericias para desenvolverse con soltura y seguridad a través de las diferentes redes, comprendiendo como se ve afectada una misión cuando colapsa el sistema de comando y control de un Teatro de Operaciones. Por ello, la estructura orgánica debe poner énfasis en lograr la familiarización de estos profesionales con el espectro completo de amenazas a los sistemas de información y las consiguientes respuestas a los posibles ataques.

3.4 Soluciones en el Mercado Tecnológico

Gracias al constante crecimiento de la tecnología, la industria dedicada al espacio cibernético adquiere día a día mayor envergadura/relevancia teniendo como misión y objetivo principal poder brindar soluciones eficientes y de bajo costo. Países como Estados Unidos, Canadá, Corea del Sur, Francia y España entre otros, es donde se puede observar un compromiso de los gobiernos y de las empresas por incentivar el desarrollo y el ámbito científico en estos aspectos.

En el campo de la seguridad y prevención de riesgos, como así también de amenazas en el ciberespacio hay una conjunto de diferentes tipos de herramientas aptas para hacer frente a la problemática. Queda fuera del alcance de la presente investigación el

59 Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España. Pág. 220.

hacer una identificación exhaustiva de las mismas, ni detallar el estado del arte de cada una de ellas, tanto en el ámbito comercial como militar[60].

Sin embargo se puede encontrar aspectos a tener en cuenta, entre los cuales hay que observar cuales son las soluciones disponibles y, entre éstas, cuales son las más extendidas, sus principales proveedores, funcionalidades y amenazas a las que están orientadas cada una de ellas; la reducción al nivel de riesgo con la que contribuyen; el costo de adquisición; el esfuerzo que lleva asociado su despliegue, así como los costos y esfuerzos para el apoyo y mantenimiento; las posibles restricciones legales y reglamentarias en función del ámbito en el que se apliquen, etc[61].

Conducido principalmente por la dependencia y necesidad que el manejo de la información impone, el mercado de la seguridad informática esta siendo testigo de un crecimiento único en la ultima década.

Con el fin de seleccionar las mejores soluciones tecnológicas es importante entender que son necesarias algunas características básicas:[62]

- **Flexibilidad y capacidad:** debe ser una herramienta con una arquitectura que permita una configuración fácil y rápida para adaptarse a unos requisitos específicos.
- **Gráficos y generación de informes:** el formato y contenido de la información se debe poder personalizar.
- **Notificaciones personalizadas:** debe ser posible configurar notificaciones y alertas para distintas situaciones, y su integración en varios canales, SMS, correo electrónico, voz, WAP-Push, etc.
- **Estabilidad y baja carga:** funcional con pocos recursos de hardware y tener tasas de disponibilidad elevadas.
- **Madurez:** la herramienta-tecnología debe estar probada y desplegada en el mercado.
- **Fácil de usar:** disponer de interfaz web que proporcione una vista rápida del estado del sistema con varias opciones o niveles de detalle.

Habiéndose planteado estas características, se puede direccionar el aislamiento y protección de redes de transferencia y procesamiento de información por medio de tecnologías, dispositivos o normas, entre las cuales se encuentran:[63]

60 Cortes Pérez, Manuel. "El Ciberespacio. Nuevo Escenario de Confrontación". Centro de Estudios del Ministerio de Defensa. España. Febrero de 2012. Capítulo VI. Pág. 293.
61 Ídem Pág. 294.
62 Ídem. Pág. 287 y 288.
63 Cortes Pérez, Manuel. "El Ciberespacio. Nuevo Escenario de Confrontación". Centro de Estudios del Ministerio de Defensa. España. Febrero de 2012. Capítulo VI. Pág. 293 - 299.

- **Cortafuegos:** permiten el filtrado de tráfico sobre las redes, bloqueando el acceso no autorizado[64].
- **Routers:** conmutadores, concentradores y cualquier otro dispositivo de comunicación y de interconexión con capacidades de filtrado.
- **Servidor proxy:** ordenador o aplicación que recibe las peticiones y conexiones de red que se hacen a un servidor de destino.
- **VLAN (Virtual Local Area Network):** red de área local virtual. Admite la creación de redes lógicas independientes, dentro de una única red física.
- **NAT (Network Address Translations):** traducción de direcciones de red. Mecanismo que usan los routers para permitir el intercambio de paquetes entre redes, asignándose entre ellas direcciones incompatibles, accediendo a internet por medio de direcciones privadas.
- **Honeypot**: software o grupo de ordenadores cuyo objetivo es atraer a potenciales atacantes, simulando ser sistemas vulnerables o débiles. Asimismo se la emplea para recoger información sobre los atacantes y sus técnicas.

Por otra parte existen herramientas que se encargan de detectar las potenciales intrusiones al ciberespacio de un estado, entre ellas se pueden mencionar las herramientas de evaluación y de detección de vulnerabilidades, como son los llamados escáneres de vulnerabilidad o analizadores de red, escáneres de puerto, que detectan si el puerto de una maquina está abierto, cerrado o protegido por un cortafuegos, y los escáneres de sistema operativo[65].

En el ámbito de la detección y protección contra virus y malware se dispone de los siguientes tipos de soluciones: antivirus y soluciones para software malicioso para equipos de sobremesa y portátiles, antivirus y soluciones de software malicioso para los servidores (gateways HTTP, servidores de correo, servidores de archivos, etc.), soluciones antispam y herramientas de verificación de integridad de archivos críticos[66].

Existen tecnologías utilizables en archivos de multimedia que se orientan al encubrimiento de la información por medio del uso de ofuscación de código o estenografía. En general, la ofuscación consiste en el proceso de encubrir la información haciéndola más confusa de leer e interpretar a través de un cambio no destructivo dentro del código fuente del programa[67]. La esteganografía, consiste el hecho de ocultar mensajes o información dentro de otros objetos, que actúan como portadores, de manera que para alguien no avisado no es capaz de detectar su presencia[68].

64 Casar Corredera, Jose R. "Tecnologías y Servicios para la Sociedad de la Información". Universidad Politecnica de Madrid. Enero 2005. Pág. 166.
65 Anonimo."Guía/Norma De Seguridad De Las Tic (Ccn-Stic-400) Manual Stic". Mayo 2013. Pág. 146.
66 Ídem. Pág. 175-178.
67 Enciclopedia Universal. Disponible en: http://enciclopedia_universal.esacademic.com/49511/Ofuscación.
68 Anónimo. "Esteganografía, el Arte de ocultar información". Instituto Nacional de Tecnologías de la Comunicación. Pág. 1. Disponible en: http://neobits.org/recursosexternos/inteco.pdf.

Una tarea importante dentro del manejo de la información y que asegura su tráfico y diseminación es mantener una copia de seguridad/respaldo o backups de toda la información almacenada en los sistemas o computadoras. Para ello se dispone de diferentes utilidades de copia de seguridad, dispositivos y herramientas de generación de imágenes.

Actualmente se cuenta con sistemas y/o tecnologías que permiten la operatividad de las áreas cibernéticas las 24 horas, sin interrupciones, vital para el traspaso de información entre las fuerzas en el área del teatro. Entre estos pueden encontrarse los clustering de servidores y el empleo de discos en espejo. Así también los sistemas RAID, de virtualización y balanceo de carga permiten mantener la operación fluida de la infraestructura informática[69].

La configuración de tráfico es una práctica de gestión de tráfico en Internet, orientada al control del tráfico de redes informáticas con el fin de optimizar las prestaciones o la garantía de servicio, mejorar la latencia y/o aumentar el ancho de banda utilizable, retrasando los paquetes que cumplen con ciertos criterios[70].

Los sistemas de información deben estar ubicados dentro de áreas que cuenten con protección electromagnética, sobre todos aquellos que manejen información critica dentro y fuera del Teatro de Operaciones. Esto puede lograrse por medio del empleo de jaulas de Faraday, las cuales se encargan de disipar las emanaciones electromagnéticas desde el interior hacia el exterior. Esta capacidad hace que la zona protegida con una jaula de Faraday disponga de una medida de protección eficaz contra los ataques TEMPEST (Transient Electromagnetic Pulse Surveillance Technology)[71].

Además existe la necesidad como soporte físico a los protocolos y todos los sistemas o herramientas anteriormente enumerados la posibilidad del empleo de tarjetas con chips individuales y personalizadas para cada usuario del sistema y que serian necesarias para garantizar el acceso al sistema integral de información, tanto en las redes de Comando y Control, como en las de Propósito General, el empleo de la firma electrónica[72].

La medida de seguridad más adoptada en general es el uso de firewalls entre redes privadas y públicas pero también es importante disponer de limitaciones de hardware o software que prohíban el uso de dispositivos de memoria flash u otros soportes extraíbles. La prohibición del uso de llaves USB y otros soportes de este tipo se ha adoptado más ampliamente en Arabia Saudí (65%) y Rusia (50%). Su adopción es mucho menos generalizada en España (13%) y Brasil (20%)[73].

---

69 Cortes Pérez, Manuel. "El Ciberespacio. Nuevo Escenario de Confrontación". Centro de Estudios del Ministerio de Defensa. España. Febrero de 2012. Capítulo VI. Pág. 298.
70 Ídem. Pág. 298.
71 Ídem. Pág. 299.
72 Anónimo. "Tarjetas Inteligentes y Sistemas de Identificación Seguros: Construyendo una Cadena de Confianza". Smart Card Alliance. U.S.A. Pág. 10 y 11. Julio 2005. Disponible en: http://www.smartcardalliance.org/latinamerica/translations/Building_a_Chain_of_Trust_Spanish.pdf.
73 Baker Stewart, Steptoe & Johnson, Waterman Shaun, George Ivanov. "En el punto de mira las infraestructuras críticas en la era de la ciberguerra. Un informe global sobre las amenazas que sufren los sectores clave". Mc Afee. Disponible en: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf.

Como se puede observar, los responsables e involucrados en temas relacionados con la seguridad en el ciberespacio, deben poseer una actitud agresiva e innovadora, esencial para el desarrollo tecnológico y poder enfrentar el cambio de paradigma en los conflictos actuales y futuros, orientando las soluciones tecnológicas a fin de garantir las características básicas del manejo de la seguridad de la información: grado de reserva, integridad y disponibilidad.

Sin embargo el estado y las Fuerzas Armadas deberían ser los que ostenten el mayor grado de responsabilidad para probar y liderar el mercado de la ciberseguridad por ser este uno de los mas permeables y sensibles a la fuga de información. Esto a su vez debería generar plataformas orientadas al sector comercial para que se nutra y crezca simultáneamente en sus capacidades y se encargue de efectuar desarrollos de manera mas accesible y económica**.**

Conclusiones

Los estados son aquellos que tienen el monopolio del empleo de la fuerza y por ello juegan un papel vital en el área de seguridad y defensa, marcando el ritmo, regulando conductas y ayudando a crear un ambiente de desarrollo seguro para la obtención de sus intereses.

La pérdida de confianza por parte de la sociedad es un costo inaceptable para un estado cuando se trata de seguridad cibernética. La falta de regulación y administración por parte de este respecto de la seguridad de información no genera otra cosa que el detrimento de la legitimidad del poder y monopolio estatal.

La creciente importancia de los sistemas de información en los ambientes de crisis, conflictos y guerras actuales revelan que la seguridad de la información es crítica para la obtención de la victoria y el desarrollo de las actividades antes, durante y posterior al conflicto.

El empleo efectivo de los medios y tecnologías cibernéticas facilitan y favorecen el dominio de las Fuerzas Armadas en un Teatro de Operaciones, siempre y cuando se sustenten en estructuras orgánicas con la adecuada distribución personal. Además contar con esta capacidad disuade al potencial enemigo de escalar una crisis por temor a la desarticulación de su centro de comando y control.

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

La dependencia tecnológica y la facilidad para acceder a las tecnologías contribuye a que aumenten las probabilidades de sufrir ataques cibernéticos y permiten a los

potenciales adversarios obtener inteligencia sobre las propias capacidades, operaciones, proyectos en desarrollo y planes estratégicos.

Contar con la capacidad de combatir y defenderse contra un ataque cibernético debería ser un objetivo primordial para el Estado nacional y una misión de las Fuerzas Armadas, para ratificar la seguridad, supervivencia, estabilidad y defensa del estado.

Es necesario para el desarrollo de medidas de seguridad, formar profesionales especializados, supervisar la aplicación de medidas de seguridad cibernética, adquisición de tecnología y contratación de servicios especializados con el respectivo análisis de riesgos ante un ataque cibernético.

El tratamiento de la información, su seguridad física y digital juntamente con el establecimiento de diferentes niveles de alarma, asegura el grado de preparación necesario para hacer frente a agresiones cibernéticas en el Teatro de Operaciones.

Es así como luego de desarrollar el trabajo de investigación y haber enunciado estas conclusiones, se puede afirmar la validez de la hipótesis planteada, sobre la importancia que tiene el desarrollo de estructuras orgánicas que aseguren el intercambio de datos, junto a la capacitación de personal en las áreas de empleo de redes y manejo de información dentro del ciberespacio permite asegurar la defensa de la infraestructura y medios militares argentinos en el Teatro de Operaciones.

Recomendaciones Finales

Sería necesario impulsar un presupuesto asignado de manera singular para lograr la implementación de estos desarrollos, tecnológicos y de personal, incentivando programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas.

Se debería tener en cuenta avanzar hacia una gestión de las redes de administración pública buscando alcanzar los requisitos mínimos de seguridad para la interoperabilidad de las diferentes agencias, asegurando de manera confiable la defensa homogénea del sistema de información.

El Ministerio de Defensa debería desarrollar un manual de procedimientos y accionar conjunto para el manejo de la información y seguridad cibernética. Este en su carácter de piedra fundamental tendría que reflejar todas las normas internas en materia de seguridad de la información del Ministerio y de las diferentes fuerzas que lo integran; de esta forma se facilitarían las coordinaciones, e interoperabilidad, permitiendo a las fuerzas desplegadas en un Teatro de Operaciones consolidar y robustecer los criterios de trabajo y empleo de los sistemas.

Se debe dotar a las redes de sistemas de análisis y correlación de registros, a fin de efectuar el monitoreo que permita obtener la necesaria alerta temprana para actuar con antelación a un incidente cibernética y reducir el impacto y alcance del mismo.

Asimismo sería indispensable la instrumentación de programas de capacitación y

concientización destinados al personal que tenga acceso a información critica o clasificada en sistemas o redes relacionados con las acciones dentro del Teatro de Operaciones y empleo los sistemas electrónicos para el procesamiento de datos, conjuntamente con una política educacional por parte del estado que potenciara el desarrollo de cátedras y jornadas en universidades y otros centros de estudios que traten la seguridad en los sistemas de información y comunicaciones.

Debido a la singularidad de la guerra cibernética y las características del ciberespacio la cooperación a nivel regional e internacional se vuelve una prioridad para los estados que pretenden alcanzar niveles eficientes de seguridad cibernética.

Resultaría imprescindible alentar el mercado nacional, profesional y de desarrollo técnico de productos, a la consecución de metas en materia de hardware y software con sus respectivas certificaciones de seguridad.

Como se ha podido ver son diversas las alternativas cuando se trata de los niveles de formación de recursos humanos en el ámbito de una agencia de seguridad cibernética. Es recomendable que estas se realizaran tanto en el ámbito local como regional e internacional, resultando fundamental la aplicación de un eficaz programa de comunicación que direccione al personal hacia la adquisición de este tipo de formación profesional.

A los fines de cumplir con un programa serio y eficiente de formación se recomienda la firma de convenios con universidades nacionales donde se dicten maestrías o especializaciones acreditadas por la Comisión Nacional de Evaluación y Acreditación Universitaria, como también en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Asimismo, el inicio de la actividad educativa en el ámbito nacional en materia de seguridad cibernética, permitiría el envío de oficiales y personal civil de las Fuerzas Armadas y administración gubernamental con injerencia en la temática, a cursar maestrías y posgrados en instituciones tales como el Naval Post Graduate School, Universidad Tecnológica de Tallin, iCollege de la National Defense University.

La ciberguerra es una de las nuevas amenazas, es totalmente asimétrica y su bajo costo operativo sumado a la gran variedad de tecnología en existencia en el mundo, hacen que nuestros posibles adversarios puedan emplear este medio para satisfacer sus apetencias significando una amenaza al Estado nacional y a sus capacidades militares.

Por ello se consideraría vital el compromiso del Estado para que se activen los desarrollos necesarios que otorguen sustento a la integridad de las redes de información dentro de un Teatro de Operaciones. Dicha integridad resulta crítica y cualquier acontecimiento relacionado con un ataque a través del ciberespacio utilizando esas redes atentaría gravemente contra la soberanía nacional poniendo en riesgo la seguridad física de los habitantes del Estado argentino.

Bibliografía

Documentos Oficiales

- Anónimo. "International Strategy for Cyberspace". Casa Blanca. Estados Unidos. Mayo 2011.

- Anónimo. "Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio". Instituto Español de Estudios Estratégicos. Ministerio de Defensa. España.

- Tritz, Gerald. "Cyberspace and the Operational Commander". Naval War College. Newport. USA. 2010.

Documentos Electrónicos

- Anónimo. "Information Operations" Agosto 1996. Department of the Army.

- Anónimo. "Tarjetas Inteligentes y Sistemas de Identificación Seguros: Construyendo una Cadenaade Confianza". Smart CardaAlliance. U.S.A. Dis ponible en: http://www.smartcardalliance.org/latinamerica/translations/Buildin g_a_Chain_of_Trust_Spanish.pdf. Julio 2005.

- Anónimo. "Pentágono advierte que los ataques cibernéticos son 'actos de guerra'". Londres. Disponible en: http://www.seguridad.unam.mx/noticias/?n oti=4646. Junio 2011.

- Anónimo. "EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán". Disponible en http://www.elmundo.es/elmundo/2012/ 06/20/navegante/1340173299.html. Junio 2012.

- Anónimo. "Guía/Norma de Seguridad de las TIC (CCN-STIC-400)". Centro Criptológico Nacional. España. Mayo 2013.

- Anónimo. "Seguridad de la Información". Ministerio de Defensa de España. Disponible en: http://www.defensa.gob.es/politica/infraestructura/seguridad-informacion/.

- Anónimo. Department of Homeland Security. Disponible en: http://www.us-cert.gov.

- Anónimo. "Esteganografía, el Arte de ocultar información". Instituto Nacional de Tecnologías de la Comunicación. Disponible en: http://neobits.org/recursosexternos/inteco.pdf.

- Acosta Oscar Pastor, Pérez Rodríguez José Antonio, Arnáiz de la Torre, Taboso Ballesteros, Daniel Pedro."Seguridad Nacional y Ciberdefensa". Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones Ciudad

Universitaria. Madrid. Octubre 2009.

- Avalos, Marco Carlos. "Ciberespacio y Cibercultura". Disponible en: gabrieldjs.wikispaces.com/file/view/Ciberespacio+y+cibercultura-1.doc.

- Baker Stewart, Steptoe & Johnson, Waterman Shaun, George Ivanov. "En el punto de mira las infraestructuras críticas en la era de la ciberguerra. Un informe global sobre las amenazas que sufren los sectores clave". Mc Afee. Disponible en: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf.

- Bejarano, José Caro. "El Control de Armas en la Era de la Información" Instituto Español de Estudios Estratégicos Disponible en: h ttp://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI28 2012_In formationAge_ArmsControl_MJC.pdf. Mayo 2012.

- Casar Corredera, Jose R. "Tecnologías y Servicios para la Sociedad de la Información". Universidad Politecnica de Madrid. Enero 2005.

- Cohen,aFred.a"Influence Operations". USA. Disponible 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.

- Cyberspace & Information Operations Study Center. Disponible 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. Disponible http://www.iprofesional.com/notas/156056-La-guerra-ciberntica-sale-de-las-computadoras-y-llega-a-la-economa-real". Abril 2013.

- Díaz Del Río Duran, Juan José. "La Ciberseguridad en el ámbito militar". Ministerio de Defensa de España. Diciembre 2010.

- Enciclopedia Universal. Disponibleaen: http://enciclopedia_universal.esacade mic.com/49511/Ofuscación.

- Ferrero, Julio Alberto. "La ciberguerra, génesis y evolución". Revista General de Marina. España. Enero-Febrero 2013.

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

- Goetz John, Rosenbach Marcel and Szandar Alexander. "War of the Future: National Defenseain Cyberspace". Disponible en: http://www.spiegel .de/international/germany/0,1518,606987,00.html. Febrero 2009.

- Ponemon Institute LLC. "Possibility Theory Framework for Security Evaluation in National Infrastructure Protection. Journal of Database

Management". Baskerville, R. L., & Portougal, V. A. Traverse City, Michigan, USA. 2003.

- Ponemon Institute LLC. "First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies". Traverse City, Michigan, USA. 2010.

- Ponemon Institute LLC. "2011 Cost of Data Breach Study: United States". Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC. Traverse City, Michigan, USA. 2012.

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

- Rozoff, Rick. "El Pentágono se asocia con la OTAN para crear un sistema de guerra ciberspacial global". Disponible en 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. Disponible en: http://www.revista-ays.com/DocsNum10/PersAAPP/salanova.pdf. 2007.

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

- Stiennon, Richard. "Surviving Cyber War". IT-Harvest. U.S.A. Disponible en: http://www.slideshare.net. April 2009.

- Srimoolanathan, Balaji. "Cyber Security – From Luxury to Necessity". Febrero 2011.

- Villarroya Quintero, José Luis. "Las TIC en el Ministerio de Defensa". Ministerio de Defensa. España. Junio 2012.

- Wasserbly, Daniel. "Cybercom formulating offensive teams". Jane's Defence Weekly. Washington. 2013.