MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

TRABAJO FINAL INTEGRADOR

TEMA:

La seguridad en el manejo de la información en el nivel operacional

TÍTULO:

El elemento de comunicaciones para la protección de la información en las operaciones militares en el teatro de operaciones

AUTOR: My (EA) Sergio Alberto Velasco

PROFESORA: Dra. Lucía Alejandra Destro

Año 2014

RESUMEN

Los avances tecnológicos en redes de telecomunicaciones e informática impulsados por países como los Estados Unidos de Norteamérica, España y en el marco regional Brasil, han sido el verdadero motor generador de los cambios dentro del ambiente operacional, pero sobre todo en los sistemas de comando, control, comunicaciones, informática, inteligencia y reconocimiento. Esto hace replantear constantemente la validez de las estructuras de las organizaciones, la doctrina militar vigente, hasta el proceso de enseñanza-aprendizaje en los institutos de formación y de perfeccionamiento de las fuerzas armadas.

En el nivel operacional dichos avances plantean un mayor desafío al operar en forma conjunta y en algunos casos hasta en forma combinada, donde la interoperabilidad del sistema de comando y control se pondrá a prueba a cada momento, pudiendo este ser vulnerado desde múltiples lugares y de varias formas.

Asimismo, obliga a reformular la forma de planificar, administrar y proteger la información dentro de un campo de combate mucho más agresivo que en tiempos pasados, donde el valor de la información para un comandante es fundamental para desarrollar y conducir las operaciones militares en todos los niveles de la guerra.

De aquí que en este trabajo el objetivo es proponer una estructura adecuada y las funciones de los elementos de comunicaciones que permitan asegurar el manejo de la información en el nivel operacional.

Palabras clave: Protección de la información. Sistema de comando, control, comunicaciones, informática, inteligencia y reconocimiento (C4ISR). Nivel operacional. Seguridad informática.

Tabla de contenidos

INTRODUCCION

En el ámbito civil y en los principales ejércitos del mundo existe una amplia bibliografía sobre los sistemas de comando, control, comunicaciones e informática y la interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control, en los distintos niveles. Estos han intentado dar una respuesta a las múltiples necesidades de la conducción y/o subsistemas componentes.

Después de la segunda Guerra del Golfo, en el ejército de EE.UU, se han adoptado una serie de normativas y procedimientos que limitan el tipo de información a transmitir y la forma de diligenciarla. Consecuentemente, se han creado distintos elementos de comunicaciones destinados a monitorear, mantener y detectar posibles fugas de información.

En el ejército de tierra de España, conscientes de esta evolución tecnológica, han implementado procedimientos operativos para la protección de la información, generando elementos especializados en telecomunicaciones y sobre todo en seguridad informática.

En el marco regional, el ejército de Brasil también está desarrollando sus normas y procedimientos específicos sobre el manejo de la información y actualmente se encuentra experimentando con elementos especiales para asegurar las comunicaciones.

En la Argentina, se ha comenzado a estudiar las normas y procedimientos que un elemento debería poseer a fin de asegurar las telecomunicaciones en el nivel operacional, pero hasta el momento no se ha generado. De aquí que cabe preguntarse ¿Qué estructura deberían tener y cuáles serán las funciones de los elementos de comunicaciones para el uso y manejo de la información en el nivel operacional?

Para dar respuesta al interrogante formulado, en esta investigación se brindan elementos de juicio y orientaciones para una posible solución a la seguridad en el manejo de la información, mediante la propuesta de un elemento que cuente con las funciones, las capacidades y una organización que le posibilite asegurar el desarrollo de operaciones militares en el nivel operacional con sustento en la doctrina, normas y procedimientos de países con experiencia en seguridad de la información en el nivel operacional del conflicto.

A modo de hipótesis se afirma que para asegurar el manejo de la información, el elemento de telecomunicaciones no puede prescindir de encriptadores, analistas, programadores y un grupo de control redes, a fin de asegurar el diligenciamiento y manejo de la información en forma segura en el campo de combate moderno.

El objetivo general de investigación se concentra en realizar el diseño de una estructura y funciones de los elementos de comunicaciones para asegurar el manejo de la información en el nivel operacional, explotando la experiencia de los ejércitos anteriormente mencionados.

Para ello se recurre principalmente al análisis bibliográfico de las fuentes doctrinales militares del Ejército de Estados Unidos, el Ejército de Tierra de España y el Ejército de la República Federativa del Brasil, tanto en forma digital como en forma escrita, a través de las distintas prescripciones reglamentarias relacionadas con el tema en cuestión.

Para lograr el objetivo general planteado, los contenidos del trabajo se encuentran organizados en tres capítulos en los que se plasman los objetivos específicos. En el primero se identifican la organización, las funciones y misiones de los elementos que brindan la seguridad de la información en el marco regional y la OTAN. En el segundo capítulo se definen normas y procedimientos para asegurar el manejo de la información. En el tercero se especifican los lineamientos y estructura de un posible elemento de comunicaciones destinado a brindar la seguridad en el manejo de la información que satisfaga las exigencias que impone el campo de combate moderno en el manejo de la información.

CAPÍTULO 1

"ORGANIZACIÓN, FUNCIONES Y MISIONES DE LOS ELEMENTOS QUE BRINDAN LA SEGURIDAD DE LA INFORMACIÓN"

1. Finalidad del capítulo

El presente capítulo desarrolla la implementación de la seguridad informática dentro del C4ISR en el ejército de los Estados Unidos y se exponen normas y procedimientos empleados en la evolución de la seguridad en el manejo de la información para extraer experiencias, conclusiones y adaptarlas a las necesidades de las fuerzas armadas en el nivel operacional.

SECCIÓN 1

TECNOLOGÍAS IMPLEMENTADAS EN LOS SISTEMAS C4ISR

Los modernos sistemas de comando y control se están desarrollando con las tecnologías emergentes en los campos de las telecomunicaciones y la informática, procedentes principalmente del ámbito civil, como consecuencia de su más avanzado estado, su mayor disponibilidad. La política de defensa y la estrategia militar reconocen la importancia y el valor de las nuevas tecnologías aplicadas a los sistemas C4I para la mejora de la eficacia y la eficiencia y, en consecuencia, se están llevando a cabo iniciativas para conocer su factibilidad de aplicación para incluir estos modernos medios y técnicas en los sistemas de comando y control operativos en el marco de la acción militar conjunta.

A modo de ejemplo podemos citar los ejercicios que realizan anualmente Estados Unidos para demostrar la capacidad operacional y la validez de las nuevas tecnologías, haciendo partícipe a empresas americanas en los sistemas de defensa. Se trata de los ejercicios de demostración JWID (Joint Warrior Interoperability Demostration) patrocinados sucesivamente por el ejército americano, con participación desde 1996 de países de la OTAN, entre ellos España, con éxito destacado. La empresa española participante desde aquella fecha ha merecido durante dos años la mención máxima por el desarrollo del WEBCOP, considerado como el sistema de comando y control más

innovador y de mejores posibilidades operativas a nivel operacional. Basados principalmente en la creación de este sistema se han utilizado herramientas comerciales WEB, adaptadas y combinadas para lograr tales resultados, PC comerciales y comunicaciones militares y civiles formando una red, protegiéndose la comunicación con equipos de criptografía OTAN.

Un inconveniente que se ha presentado es la rapidez con que se suceden y desarrollan nuevas tecnologías lo cual conlleva su pronta obsolescencia y obliga a establecer un compromiso en la modernización / renovación de los sistemas y equipos; es decir, agotar al máximo los ciclos de vida o modernizar / sustituir, aplicando las tecnologías más avanzadas. El uso de las mismas sirven fundamentalmente para mejorar la eficacia operativa en el desarrollo y conducción de operaciones militares adquiriendo aún mayor complejidad cuando se desarrollan en el ámbito conjunto o combinado e implica la renovación de la doctrina de empleo.

Señalemos ahora que los sistemas C4I deben facilitar a las unidades de los distintos ejércitos cumplir las misiones conjuntas y combinadas que se les asignen y operar entre sí sin problemas de entendimiento, pasando a analizar sus más relevantes características: La interoperabilidad, la seguridad de empleo operativo, la flexibilidad y la actualización cultural del personal y de la organización en las nuevas tecnologías. Directamente relacionado con la tecnología, surge el concepto de seguridad que será requerido por el sistema de información definiendo niveles de clasificación e imponiendo la utilización de servidores de control de accesos. Los cuales permiten el monitoreo de los usuarios y obtienen información del sistema. Asimismo, la utilización de software de control de acceso a la red de área extendida (Firewalls) lo que permite el control de accesos desde el exterior de la red, además de detectar posibles ataques al sistema.

Para lograr comprender como las fuerzas armadas de los Estados Unidos han organizado el sistema de comando, control, comunicaciones y computación para lograr asegurar el manejo de la información, a continuación se desarrolla un cuadro explicativo extraído del reglamento FM 6-0 Mission Command: C2 of Army Forces, HQ Department of Army, 2003, Chapter 5.

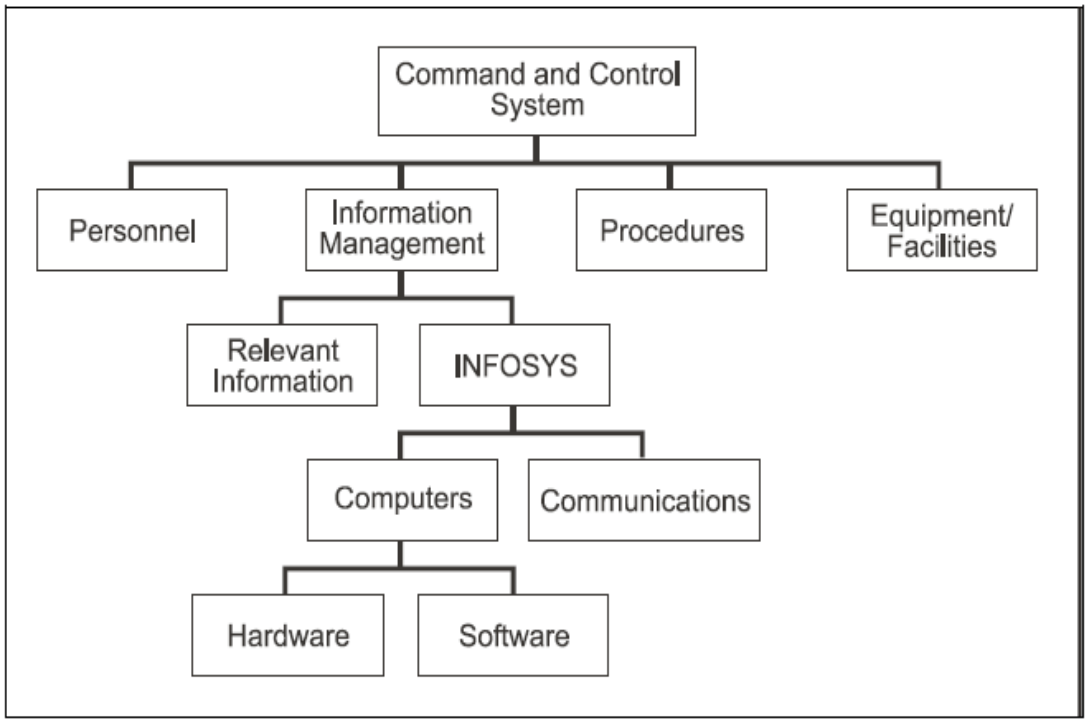

Figure 5-1. Elements of the Command and Control System

A continuación se describe las funciones que cada elemento desarrolla para asegurar el manejo de la información en su zona de responsabilidad.

El elemento "personal" posee una capacitación técnica específica (Ingenieros informáticos y en diagnóstico de redes de informática, analistas y programadores, auditores de redes) delineando un perfil requerido para el desarrollo de sus tareas específicas. Los "procedimientos" se especifican doctrinalmente en los distintos reglamentos y manuales para el empleo de los sistemas C2 y se detallan a nivel de Standard Operating Procedure (SOPs), según el Comando de trabajo.

Los "equipos y facilidades". Reúne todo lo necesario relacionado con materiales y equipos para desarrollar la actividad (vehículos, cabinas, instalaciones y materiales para los servicios logísticos para racionamiento, sanitario, transporte, etc.), sistemas informáticos y de comunicaciones internas. Las facilidades cumplen diferentes funciones: protección, servidor para centro de datos, sala de reuniones y para videoconferencias, medios para exposición de información (pantallas, mesas de arena, cartas).

El elemento "gestión de la información" (Information Management - IM). Su finalidad es gestionar y controlar la información tanto la que entra como la que

diligencia hacia otros elementos en sus respectivas zonas de jurisdicción. Apoyados en el gráfico vemos que se subdivide en dos subcomponentes: "Relevant Information (RI)" & "Information System (INFOSYS)".

Information System: INFOSYS son los equipos y facilidades que recogen, procesan, almacenan, muestran y diseminan información. Se compone a su vez de sistemas informáticos y sistemas de comunicaciones. Como sistema soporte, el elemento INFOSYS está vinculado directamente con la forma de procesar o diligenciar la información, siendo vital para ello la determinación de normas y procesos de automatización y diligenciamiento que liberen a los usuarios del sistema y al decisor de tareas menores.

La arquitectura general del INFOSYS, se integra en varios niveles, incluyendo el Sistema Nacional Conjunto (Global Command & Control System (GCCS)) con interface al Sistema de Campaña (Army Battle Command System (ABCS))[1].

SECCIÓN 2

IMPLEMENTACIÓN DE LAS NUEVAS TECNOLOGÍAS INFORMÁTICAS EN EL MANEJO DE LA INFORMACIÓN.

Un aspecto que es necesario destacar y que está directamente relacionado con las actividades de la Defensa Nacional, principalmente con la acciones en tiempos de paz, es la implementación de las redes sociales para mejor respuesta social ante las grandes catástrofes como pueden ser de ataques terroristas, y desastres naturales o situaciones de emergencia social, como así también, en la notificación de estos eventos mediante la utilización de las redes sociales de manera de acotar los tiempos de respuesta, apelando a su capacidad de transmisión instantánea de la información y a la flexibilidad que éstas ofrecen tanto en el ámbito civil como militar.

Las fuerzas armadas norteamericanas desarrollan ejercicios que se realizan anualmente a cargo de la "Agencia Federal para el Manejo de Emergencias, el Departamento de Seguridad Nacional (DHS), el Departamento de Defensa, varios

[1] US Army; Mission Command: C2 of Army Forces, HQ Department of Army; FM 6-0, Edition 2003, Chapter 5.

gobiernos estatales y locales y muchos otros"[2]. En el nivel nacional tienen como finalidad "mejorar la respuesta nacional a las grandes catástrofes, como terremotos, ataques terroristas e incidentes nucleares"[3].

En su ejecución, se puede comprobar el funcionamiento de las redes de telecomunicaciones militares como las sociales en conjunción con las telecomunicaciones públicas en dos momentos fundamentales en las catástrofes, el antes y el después de su ocurrencia.

En este sentido, el Jefe de la Dirección de Sistemas de Transformación Battlespace en Picatinny Arsenal, Gene Olsen ha sostenido que:

> … "Nos dimos cuenta de que habrá una enorme participación de las redes sociales para algo como esto. Las redes sociales nos puede ayudar después de ocurrido un desastre, si se relacionan con los sistemas existentes Departamento de Defensa y el Departamento de Seguridad Nacional, ya que podrían ayudar a coordinar los esfuerzos de respuesta"[4]...

Hasta ahora, solo las redes militares adoptaban previsiones para lograr una rápida respuesta ante hechos de seguridad en su ámbito específico y conjunto, pero las redes sociales se habían observado desde el punto de vista posterior a la ocurrencia de un hecho puntual para la interacción y transmisión de las noticias e información. A raíz de ello actualmente se está comenzando a valorar las redes sociales en su potencial en la predicción de determinados eventos, lo que contribuirá en la oportuna adopción de decisiones, junto con la interconexión con los sistemas del Departamento de Defensa y el de Seguridad Nacional.

El ejército de Estados Unidos ha implementado un sistema complejo denominado Global Information Grid (GIG)[5], que opera tanto en guarnición como en tiempo de guerra, sobre un conjunto de capacidades y facilidades de información que permiten en forma global de comunicación punto a punto, como vector válido para la recolección, procesamiento, almacenamiento y difusión de la misma. Esta malla global de terminales

---

2 Seffers George I., Signal Online Exclusive, December 19, 2011; Recuperado de *http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2830&zoneid=334.* 03/Ago/2012.
3 Ibidem.
4 Ibidem.
5 Us Army; Joint Publication 6 – 0 Joint Comunications Systems. Chapter II, p. 40.

y facilidades de telecomunicaciones incluye tanto las propias (sistemas destinados a fines específicos como los provenientes de sistemas territoriales y subsidiarios) constituyendo para la Estrategia Nacional y Militar una necesaria interface a usuarios multinacionales de cooperación estratégica. En el plano específicamente de la estrategia operacional permite potenciar la acción conjunta y la interacción y enlace con los niveles decisores superiores buscando, además, el acceso redundante e ininterrumpido a la información por parte de este.

Las características de este sistema se pueden concretar en la unidad de mando y comando, políticas y normas comunes, autenticación de sistemas globales, control de acceso y directorio de servicios, infraestructuras, soportes comunes e información.

… "La estructura de malla reconoce siete estamentos componentes, a saber:

1) Warrior Component (Componentes Operacionales en el TO): A través de enlaces desde y hacia los sistemas de comunicaciones particulares.

2) Global Applications (Aplicaciones estandarizadas a nivel global): Conjunto de aplicaciones (medios y procedimientos estandarizados) utilizados por las fuerzas del TO.

3) Computing (Sistemas Informáticos): materializado por el subsistema informático (software y hardware).

4) Communications (Comunicaciones): Constituye el vector principal esencial sobre las facilidades y formas de explotación.

5) Foundation (Bases doctrinarias): Permiten el acceso y manejo de la información conforme a procedimientos predeterminados, disposiciones y órdenes.

6) Information Management (Gestión de la Información): Constituye la materialización de la secuencia lógica del ciclo de inteligencia.

7) Netops (Seguridad de la red): Permite la administración segura de la red y sus diversas aplicaciones con un nivel de seguridad aceptable"[6]...

Al analizar los distintos usos de las redes de telecomunicaciones en modernos sistemas de comando y control, como así también en las redes sociales para

[6] Us Army; Joint Publication 6 – 0 Joint Comunications Systems. Chapter II, p. 7.

determinar su influencia en las actividades militares se pueden extraer las siguientes conclusiones:

Durante el desarrollo de las operaciones de combate secretas, la experiencia del ejército de Estados Unidos indica que la utilización de las redes tanto militares como sociales han sido unas de las causas para poner en peligro la operación o develarla.

Lo más importante a tener en cuenta en este análisis es que la fuga de información puede surgir desde múltiples lugares a causa del personal que se encuentra directamente involucrado en la operación, también por algún familiar o integrante del círculo íntimo, o por algún actor externo que adrede o no, publique cierta información que devele la operación, por la simple necesidad social de comunicarse.

Las redes sociales y redes de área local de telecomunicaciones de elementos desplegados en un teatro de operaciones han sido de mucha ayuda a las actividades de combate, facilitando en el intercambio de información desde la óptica del combatiente individual en primera persona y mantener a las familias en contacto intercambiando información de manera segura y en un tiempo adecuado.

En las actividades administrativas y/o guarnicionales, las redes de telecomunicaciones han demostrado ser sumamente útiles en el manejo de la información cotidiana, en el diligenciamiento de documentos, cartografías, datos y su registro, en la organización de actividades guarnicionales, en la obtención de información para mejorar la calidad de vida, en el manejo de la información en forma instantánea. Pero asimismo han impuesto la necesidad de generar elementos destinados a brindar la seguridad en el diligenciamiento de la misma con capacidades y funciones técnicas específicas que en años anteriores no eran tenidas en cuenta. Siendo las transgresiones a las medidas de seguridad en la publicación de información constituye un aspecto a considerar permanentemente por los comandos y sobre todo en el nivel operacional, mediante la educación, instrucción y adiestramiento del personal y luego apelando al autocontrol, ya que no sería conveniente prohibir esta fundamental herramienta comunicacional, por lo contrario, se debe explotar y concientizar sobre su uso e implementación adoptando las medidas necesarias para evitar la fuga de información y develar el desarrollo de las distintas operaciones a cumplir.

Actualmente, tanto las redes militares dentro de un área de responsabilidad como las redes sociales en el ámbito civil, no sólo son sumamente útiles luego de algún hecho o evento para el manejo de la información, sino que pueden ser útiles para predecir y reaccionar ante una amplia gama de catástrofes, incluidos objetivos de alto valor estratégico, ataques terroristas, desastres naturales y brotes de enfermedades, tendiendo a integrarlas a las redes relacionadas con cuestiones de defensa y en nuestro caso particular al nivel operacional.

SECCIÓN 3

NORMAS Y PROCEDIMIENTOS PARA ASEGURAR EL MANEJO DE LA INFORMACIÓN

Utilización de las redes informáticas y parámetros para su regulación en el ejército de los Estados Unidos de Norteamérica

Otro parámetro necesario a analizar para brindar la seguridad de la información está relacionada con el uso de redes sociales y su empleo en el desarrollo de operaciones militares en el nivel operacional a fin de comparar experiencias de los Estados Unidos y determinar normas, procedimientos, requerir medios y determinar un elemento organizado, adiestrado y equipado que contribuya con este objetivo.

Esta necesidad y la experiencia en misiones de paz en el marco internacional han impuesto operar en forma conjunta o combinada, con países amigos y aliados.

El Departamento de Defensa de los Estados Unidos de Norteamérica, consciente de que esta revolución de las redes sociales y su influencia en el desarrollo de operaciones y cómo pueden / afectan la seguridad de la nación, ha publicado el 25 de febrero de 2010 una "Directiva denominada *"Responsabilidades y efectivo uso de capacidades basadas en Internet DTM 09-026"*[7], la cual proporciona los lineamientos generales para el uso de las redes sociales por parte del personal militar; ya que las capacidades que brinda internet están relacionadas con el Departamento de Defensa de los Estados Unidos de Norteamérica.

[7] DTM 09-026, Directiva Tipo Memorándum, Responsabilidades y efectivo uso de capacidades basadas en Internet, Secretario de Defensa, 25 Febrero 2010.

El Departamento de Ejército, con fecha del 1 noviembre de 2010, publicó un memorándum con el propósito de estandarizar la vasta presencia oficial externa del Ejército en las redes sociales, firmado por el Director de la División Online y redes sociales de la oficina del Jefe de Asuntos Públicos.

Este memorándum determina una cierta cantidad de regulaciones para la presencia en las redes sociales como Facebook, Twitter, Flickr, YouTube, blogs y cualquier otra plataforma a saber:

- "… Debe ser categorizado como una página del gobierno.
- Incluir los nombres del comandante y logo autorizados (es decir, 1 ª Brigada, 25 División de Infantería [Preparación para la Familia]), no apodo ni la mascota (es decir, no el "dragones").
- Imagen de marca (nombre oficial y el logotipo) en todas las plataformas de medios sociales (por ejemplo, Facebook, Twitter) son uniformes.
- Incluir una declaración que reconoce esta es la " la página oficial [Facebook] de [entrar a su unidad o el nombre de las organizaciones de aquí] [Preparación para la Familia]"
- Las páginas de Facebook hay por defecto para la campaña.
- Las páginas de Facebook debe incluir las "Directrices de Publicación" en el marco del uso de políticas del Ejército de EE.UU. Facebook como una referencia y / o visitar el Departamento de Defensa Social de las Condiciones de uso de medios en "ficha Información.": Http://www.ourmilitary.mil/user_agreement.shtml
- Ser reciente y actualizada. Post no debe ser mayor de un mes.
- Cumplir con las directrices de operaciones de seguridad. FRSAs / FRG líderes deben proporcionar a todos los administradores de páginas y de los miembros del FRG con el Ejército de los EE.UU. presentación de Medios de Comunicación Social OPSEC y el Informe de FBI en el robo de identidad se encuentra en el sitio slideshare del Ejército de EE.UU. en www.slideshare.net / usarmysocialmedia.
- No se debe utilizar como un lugar para la publicidad personal ni respaldo.

- Todas las páginas deben estar registrados a través del Ejército de los EE.UU. en www.army.mil / socialmedia"[8].

La oficina de asuntos públicos puede denegar la aprobación de cualquier página web y/o página oficial si no cumple con algunas de las cláusulas anteriormente mencionadas, en el ámbito nacional esta norma todavía no está regulada.

La oficina de asuntos públicos también brinda una página del departamento de defensa con instructivos para la confección y administración correcta de los sitios en cuestión.

A continuación se mencionan las partes de este instructivo que es la columna vertebral para el establecimiento de normas y procedimientos a seguir en el establecimiento / uso de redes informáticas.
Aspectos a analizar:

- Lista de chequeo para la seguridad de las operaciones.
- Establecimiento y mantenimiento de la presencia del Ejército en las Redes Sociales.

A continuación se enumeran los aspectos para incrementar la seguridad en la utilización de las redes sociales a tener en cuenta por las organizaciones y la comunidad usuaria, apoyándonos en el manual de redes sociales del Ejército de los Estados Unidos (Año 2010).

… "Lista de chequeo para la seguridad de las operaciones.

- Designar miembros responsables para publicar contenidos oficiales en línea y estar seguros del cumplimiento de las Operaciones de Seguridad.
- Asegurarse que los contenidos se encuentren aprobados por el comando de la organización.
- Asegurarse que los contenidos publicados se encuentren en concordancia con las regulaciones de la guía de asuntos públicos y del ejército.
- Monitorear la que presencia en las redes sociales de publicaciones de usuarios externos no revelen información sensible en las páginas oficiales. Monitorear el muro de Facebook, los comentarios colocados en YouTube, Flickr y blogs.

[8] Memorándum del Departamento de Ejército, estandarización de la presencia oficial externa del ejército en las redes sociales, Director de la División Online y redes sociales de la oficina del Jefe de Asuntos Públicos, de fecha del 01 noviembre de 2010.

- Distribuir las políticas de Operaciones de Seguridad a las familias de los soldados. Es importante mantenerlos actualizados al igual que los soldados de la unidad.

- Estar en alerta. Nunca sea complaciente cuando se trate de Operaciones de Seguridad. Controlar las violaciones a las Operaciones de Seguridad acerca de la presencia en las redes sociales de la organización. Nunca se termina el trabajo de proteger las Operaciones de Seguridad. Una vez que la información se encuentra publicada, no se puede recuperar"[9]...

CONCLUSIONES PARCIALES

Los ejércitos, a través de la incorporación de las nuevas tecnologías y haber adoptado de una serie de contramedidas de inteligencia en el manejo de redes sociales, han logrado disminuir el riesgo de la fuga de información tanto en las redes de telecomunicaciones militares como a través de las redes sociales, asumiendo que la necesidad de los individuos en relacionarse con sus pares es natural, y que esta comunicación la ejecutará acompañado por los adelantos tecnológicos de los que disponga.

La concreción de estas normas y procedimientos junto con la necesidad que imponen al generar elementos destinados a brindar la seguridad en el manejo de la información, es de fundamental importancia debido a los roles que desempeñan las fuerzas armadas y al riesgo que estas fugas de información representan en el campo de acción, anexados a los intentos del oponente para obtenerla.

Por otro lado, al analizar lo que ocurre con las redes militares y sociales en el ejército de Estado Unidos permite orientar el estudio y ver si es factible su aplicación en el sistema de comando, control y comunicaciones en el nivel operacional.

En base de sus experiencias comprobadas, podemos inferir que la utilización de las redes militares como de las redes sociales no solo son fundamentales en la obtención de información de la comunidad, militar o no, sino también para brindar información de utilidad en forma rápida y confiable, en la paz y en la guerra, favoreciendo no sólo la conducción de operaciones militares, y sobre todo en el ámbito de la acción conjunta.

Para adquirir la compatibilidad de un moderno sistema C4ISR y la necesidad de telecomunicación social a través de las distintas redes desplegadas, es necesario lograr

[9] Manual de redes sociales del Ejército de los Estados Unidos de Norteamérica. Enero 2011.

crear conciencia de las medidas de contrainteligencia en el personal de las fuerzas armadas a través de cursos de capacitación y adiestramiento, debido a que no podemos afirmar que los sistemas de vigilancia y control de las telecomunicaciones sean altamente desarrollados el hombre termina siendo habitualmente el eslabón más débil de la cadena.

La presente sección nos ha brindado las siguientes conclusiones:

1) No es conveniente utilizar la información relacionada con actividades operacionales, ejercitaciones, fotos de zonas sensibles que puedan comprometer la seguridad de las operaciones en desarrollo o futuras.

2) Concientizar a todo el personal sobre medidas de contrainteligencia relacionadas con la protección de datos grupales y personales, crear un grupo responsable para actualizar datos y contenidos de páginas oficiales en las redes sociales.

3) Individualmente se debe ser cuidadoso de no aceptar en la red social a personas desconocidas o no reconocidas como usuarios de la red.

4) Se deben realizar controles sobre las publicaciones de los integrantes de la Unidad / Subunidad, a fin de detectar transgresiones a las medidas de seguridad de contrainteligencia.

5) Reflejar la importancia que esta cuestión tiene para del Ministerio de Defensa del país mencionado debido a que a partir del año 1998 se creó el Comando Conjunto de Pruebas de Interoperabilidad (JITC), cuyo objetivo es la evaluación y certificación de aptitud y factibilidad técnica de las tecnologías utilizadas, tanto en el ámbito comercial como en el de Fuerzas Armadas de otros países, que permitan la interacción concurrente con el sistema de defensa de la nación[10].

6) La importancia de generar un elemento de comunicaciones destinado al monitoreo, análisis y registro de la información.

Podemos concluir, a modo de corolario, que mediante claros procedimientos y normas de empleo de los distintos sistemas de telecomunicaciones e informáticos en el uso de sus redes operacionales y guarnicionales, el usuario conoce sus libertades y

[10] Department of Defense – DISA (Defense Information System Agency). Año1998.

limitaciones en el uso de las mismas en las distintas situaciones. Asimismo, por lo expresado con anterioridad es necesario generar un elemento con capacidades técnicas que le posibiliten el manejo seguro de la información en la zona de responsabilidad, antes, durante y después de las operaciones militares previstas.

CAPÍTULO 2

"LINEAMIENTOS Y ESTRUCTURA DE UN POSIBLE ELEMENTO DE COMUNICACIONES DESTINADO A BRINDAR LA SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN"

1. Finalidad del capítulo

Determinar las características más adecuadas a las necesidades del nivel operacional de un elemento de comunicaciones destinado a brindar seguridad en el manejo de la información.

SECCIÓN 1

LAS CARACTERÍSTICAS TÉCNICAS DEL SISTEMA DE COMANDO, CONTROL, COMUNICACIONES Y COMPUTACIÓN Y LOS CONOCIMIENTOS DE LOS USUARIOS

La siguiente sección tiene por finalidad desarrollar algunos conceptos sobre sistemas de comando y control y aspectos de interés para delinear los conocimientos de los operarios de los modernos sistemas C4ISR, para lo cual se analiza un artículo realizado por el General de División (R) Benjamín Michavila Pallarés.

En el desarrollo del artículo del autor mencionado, indirectamente se hace alusión, entre otros, a conceptos como interoperabilidad, seguridad, confiabilidad claramente definidos en la doctrina de las fuerzas armadas de la República Argentina, pero en algunos temas como seguridad informática, capacidades y funciones que deben de tener los elementos destinados a brindar seguridad informática no quedan del todo abarcados.

La tarea prioritaria de las Fuerzas Armadas es la disuasión de los conflictos y, en último caso, luchar y ganar las guerras en las que se vea involucrada la nación. Asimismo, deben estar preparadas y dispuestas para participar en actividades de apoyo al restablecimiento de la paz en regiones de interés nacional, en ayuda humanitaria y en catástrofes de alcance nacional o internacional.

Operarán de forma conjunta los tres ejércitos (aire, tierra y mar) y la experiencia reciente dice que casi todas las misiones serán en combinación con fuerzas armadas de países amigos y aliados. Seguramente, para realizar la mayor parte de sus actuaciones se requiera la proyección de la fuerza a zonas alejadas.

Para facilitar el complejo y difícil ejercicio del comando, los responsables disponen de personal, organización, método y medios, componiendo el conjunto que conforma lo que se conoce habitualmente, dentro del campo profesional, como sistemas C4I, es decir: comando, control, comunicaciones, computación e inteligencia, y en el más alto nivel de la OTAN se identifica como C3 para ejercer las funciones de comando, consulta y comunicaciones. Pero, a pesar de tantas siglas como se han ido incorporando, en esencia es un sistema de comando[11].

Por lo expresado por el autor mencionado, se puede observar que la acción conjunta en el marco regional y mundial es una realidad de todas las fuerzas armadas, donde conceptos como la interoperabilidad, la seguridad y la acción conjunta entre otros conceptos serán de suma importancia en el empleo del instrumento militar, por lo que es prioritario contar con un sistema de comando y control moderno y seguro para el intercambio de información de todo tipo.

Luego, el General (R) Pallarés también sostiene que el campo de combate moderno impondrá nuevas exigencias razón por la cual los elementos encargados de asegurar en lugar y en oportunidad las telecomunicaciones deberán adoptar normas y procedimientos que faciliten la toma de decisión, con la finalidad última de dejar establecida la necesidad de la interoperabilidad de los sistemas, teniendo en cuenta la doctrina vigente y la experiencia de otros países estudiados.

[11] Michavila Pallarés Benjamín, General de División (R) – España, **"**Los Sistemas de Comando (C4I) y la Defensa**",** p. 1. Recuperado de *http://www.afcea.org.ar/publicaciones/comando.htm*

Arribó a la siguiente conclusión: Se puede decir que los avanzados sistemas de comando C4I y las modernas tecnologías ofrecen el potencial de empeñar las fuerzas militares con la mayor eficacia posible. Tanto es así que en un principio se les denominó «multiplicadores de la Fuerza». Pero, si este potencial se quiere poner en práctica, será necesario conocer las vulnerabilidades existentes en la seguridad de los sistemas de información, establecer los mecanismos para facilitar su interoperabilidad y preparar la cultura para la nueva era de la información. Solamente con las debidas acciones mantenidas en el tiempo se podrá conseguir el resultado deseable.

Lo que el General (R) Pallarés, denomina "multiplicadores de la fuerza", en la doctrina argentina se conoce como conceptos rectores de comunicaciones entre los cuales por similitud podemos mencionar: confiabilidad, seguridad, economía, flexibilidad, integración e interoperabilidad entre otros, por lo que arribamos a una primera conclusión: Debe haber un elemento de telecomunicaciones con capacidades técnicas específicas destinadas a asegurar el manejo de la información, tanto en el ámbito conjunto como combinado en el marco de la OTAN y en las distintas misiones de paz donde deba participar un elemento de las fuerzas armadas argentinas.

SECCIÓN 2

CONOCIMIENTOS NECESARIOS DEL PERITO INFORMÁTICO

En la sección anterior se ha desarrollado la tendencia evolutiva de los sistemas de comando y control, como así también una visión de cómo los avances tecnológicos imponen nuevas exigencias a los elementos encargados de brindar el apoyo de telecomunicaciones en el campo de combate moderno, a través de la visión del artículo del General (R) Pallarés del ejército de España, que junto con lo desarrollado en el capítulo I, relacionado con normas y procedimientos empleados en el ejército de los Estados Unidos, nos damos cuenta que no existe un elemento de telecomunicaciones, en nuestra doctrina actual, cuyos integrantes sean los responsables en temas relacionados con la seguridad y manejo de la información a través de medios de informáticos. Por lo cual sería necesario desarrollar un perfil informático para realizar las tareas específicas a fin de brindar los niveles de seguridad informática para el diligenciamiento y seguridad de la información, y la detección de posibles fugas de la misma.

La Dirección de Comunicaciones e Informática del Ejército Argentino ha propuesto el perfil de un perito informático acorde a las necesidades detectadas hasta la actualidad para el manejo de la información y a continuación se mencionan:

- Conocimiento sobre el mercado informático.
- Conocimiento de hardware, lenguaje de programación, sistemas operativos y manejo de herramientas.
- Conocimientos profundos sobre el marco legal vigente.
- Consideración de todos estos elementos al momento de elaborar – evaluar los puntos de la tarea pericial.
- Análisis y estudio de los puntos de pericia (expertise y experiencia requeridos).
- Especificidad vs especialidad y conocimientos técnicos del perito. Tratamiento de excepción o remoción del perito [12].

Así como hemos hecho mención al perfil que el Ejército Argentino requiere a sus peritos en informática, también en el proyecto de la Dirección de Comunicaciones e Informática se hace mención a las herramientas que se deben conocer para desempeñarse en este grupo de trabajo y que a continuación se mencionan:

Herramientas del cómputo Forense:

Sleuth Kit (Forensics Kit).
Py-flag (Forensics Browser)
Autopsy (Forensics Browser for Sleuth Kit).
dcfldd (DD Imaging Tools command line tool and also works with AIR).
Foresmost (Data Carver command line tool).
Air (Forensics Imaging GUI).
Md5deep (MD5 Hashing Program).
Netcat, crytcat (command line).
NTFS-Tools
qtparted (GUI Partitioning Tool).
Viewer.

[12] Ejército Argentino; Proyecto de la Dirección General de Comunicaciones e Informática; Edición 05 de Octubre de 2011; p 8. Recuperado de *www.cominf.ejercito.mil.ar*

X-Ways WinTrace.

X-Ways WinHex.

X-Ways Forensics.

R-Studio Emergency (Bootable Recovery Media Maker).

R-Studio Network Edition.

R-Studio RS Agent.

Net resident. Faces, encase, snort, helix.

Herramientas para el análisis de discos duros.

Access Data Forensics Toolkit (FTK).

Guidance Software Encase.

Herramientas para el análisis de redes.

E-detective – decisionComputer group Silent Runner – Accessdata.

Herramientas para el análisis de correo electrónico.

Paraben.

Herramientas para el Análisis de Vulnerabilidades.

Nessus – Retina – Nmap – Languard – Spybot.

Herramientas para filtrar y monitorear el tráfico de una red tanto interna como a internet.

Ethereal – CPA – Wireshark – Otros.

Herramientas para Análisis de USB.

USB Deview [13].

Este perfil establecido como punto de partida por la Dirección General de Comunicaciones e Informática, nos damos cuenta que es una necesidad que la estructura orgánica, evolucione e introduzca cambios en sus cuadros de organización de los elementos de telecomunicaciones para que puedan desarrollar tales funciones y tareas.

[13] Ejército Argentino; Proyecto de la Dirección General de Comunicaciones e Informática; Edición: 05 de Octubre de 2011; p. 9. Recuperado de *www.cominf.ejercito.mil.ar*

SECCIÓN 3

CAPACIDADES Y LIMITACIONES DE LOS ELEMENTOS DE COMUNICACIONES EN EL NIVEL OPERACIONAL

En el desarrollo de la siguiente sección vamos a mencionar las capacidades y limitaciones con que cuentan hoy en día los elementos de telecomunicaciones de las fuerzas armadas, de acuerdo con lo que establece la doctrina actual en las fuerzas armadas; como así también algunos conceptos de elaboración propios sobre cuáles serían las capacidades que se deberían incrementar en mencionado elemento para satisfacer las exigencias de nuevas tecnologías sobre todo en lo referente al manejo de la información a través de sistemas de telecomunicaciones e informáticos en el nivel operacional, apoyado por un proyecto que se encuentra en estudio por la Dirección de Comunicaciones e Informática del Ejército Argentino.

Considerando que es importante destacar en este capítulo el concepto de facilidades de teleinformática, que establece el ROD 05-01 que la define como:

> Equipos, seres vivos e instalaciones capaces de contribuir al envío o recepción de información de un punto a otro, los cuales, adecuadamente combinados, constituyen equipos de telecomunicaciones e informáticos con la capacidad de transmitir y recibir signos, señales, escritos, imágenes, sonidos o información de cualquier naturaleza[14].

En la definición mencionada precedentemente se puede inferir que es necesario contar no solo con equipo y material de última generación para brindar la seguridad en telecomunicaciones, sino que se deberá contar con personal altamente capacitado y con un determinado perfil que le permita cumplimentar las exigencias que, en nuestro caso, la seguridad informática imponga a los integrantes de ese elemento de telecomunicaciones en el nivel operacional.

En la actualidad, esto se logra parcialmente a través de la utilización de equipos radioeléctricos encriptados, pero en la transmisión y recepción de video e imagen todavía no se cuenta con un medio seguro, confiable e interoperable, y en la doctrina del

[14] Ejército Argentino; Conducción de Comunicaciones; ROD 05 – 01; Edición: 2001; capítulo I; artículo 3001; p. 7.

ámbito conjunto aún está en desarrollo y experimentación aunque no tiene desarrollada esta capacidad**.**

A continuación, mencionaremos algunas de las capacidades que le han sido impuestas por doctrina donde no se especifican responsabilidades respecto a la seguridad de la información a los distintos elementos de telecomunicaciones.

1. Capacidades de la Subunidad de Comunicaciones de Brigada:

El reglamento de la Subunidad de Comunicaciones de Brigada establece en el artículo 1.004 para la subunidad de comunicaciones independiente, tendrá las siguientes capacidades[15]:

a. Instalará, operará y mantendrá:

1) Dos centros de comunicaciones, uno en apoyo al Puesto Comando Principal y otro del Puesto Comando de Retaguardia de la GUC.
2) Dos estaciones terminales y dos estaciones repetidoras de radiomulticanal.
3) Tres redes radioeléctricas con el comando superior y dos redes radioeléctricas con los elementos dependientes.
4) El sistema alámbrico del Puesto Comando Principal y del Puesto Comando de Retaguardia de la GUC y con los elementos dependientes.

2. La Organización de la Subunidad de Comunicaciones de Brigada:

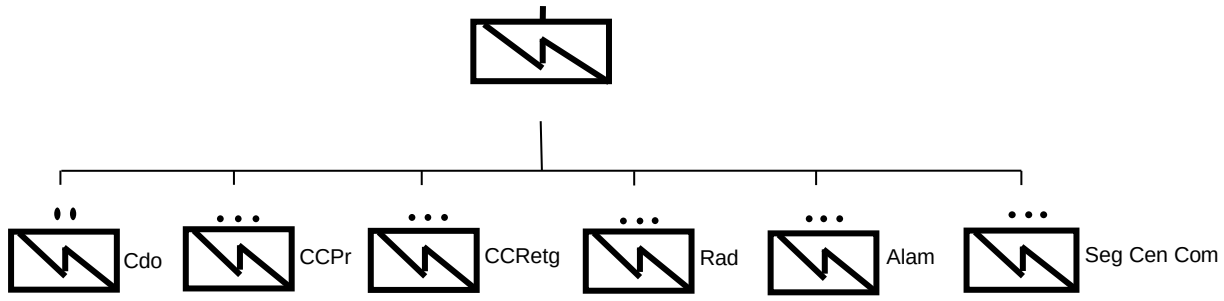

Gráfico Nro: 1 Organización de la Subunidad de Comunicaciones de Brigada**[16]**.

[15] Ejército Argentino; Conducción de la Compañía de Comunicaciones de Brigada; ROP 05-07; Edición 1997; capítulo I; artículo 1004; p. 1.
[16] Ejército Argentino; Conducción de la Compañía de Comunicaciones de Brigada; ROP 05-07; Edición: 1997; Anexo 1; artículo 1001; p. 49.

3. Capacidades del Batallón de Comunicaciones:

El reglamento del Batallón de Comunicaciones establece en el artículo 1.004 lo siguiente para el batallón de comunicaciones, tendrá las siguientes capacidades[17]:

a. Instalará, operará y mantendrá:

1) Dos centros de comunicaciones, uno en apoyo al Puesto Comando Principal y otro del Puesto Comando de Retaguardia de la GUB.

2) Una estaciones terminales y tres estaciones repetidoras de radiomulticanal.

3) Cuatro redes radioeléctricas con el comando superior y tres redes radioeléctricas con los elementos dependientes.

4) El sistema alámbrico del Puesto Comando Principal y del Puesto Comando de Retaguardia de la GUB.

4. La Organización del Batallón de Comunicaciones:

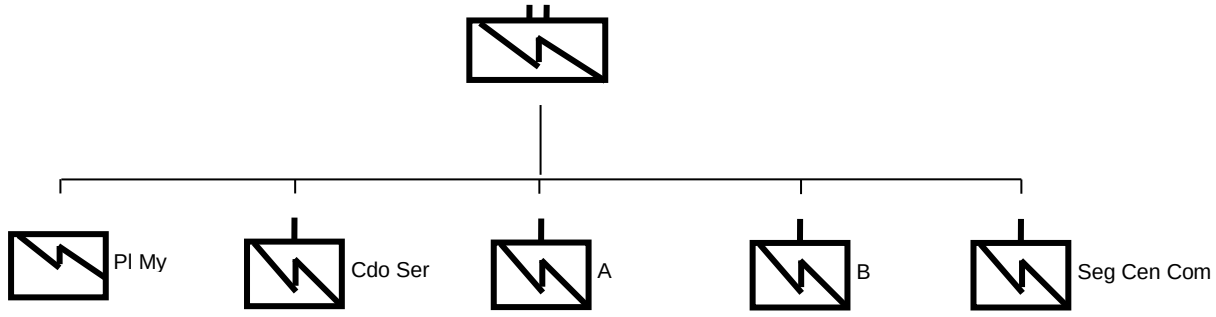

Gráfico Nro: 2 Organización del Batallón de Comunicaciones[18].

5. Capacidades de la Jefatura VI – Comando, Control, Comunicaciones, Inteligencia y Guerra Electrónica (C3 I GE):

La Jefatura VI - C3 I GE entenderá en todos los aspectos relacionados con el Comando, Control, Comunicaciones, Informática y Guerra Electrónica en el Nivel Estratégico Militar (NEM), para asesorar y asistir a las resoluciones del JEMCFFAA, a fin de contribuir a la eficacia en el accionar del Instrumento Militar (IM) de la Nación.

[17] Ejército Argentino; Conducción del Batallón de Comunicaciones; ROP 05-05; Edición 1998; capítulo I; artículo 1004; p. 1.

[18] Ejército Argentino; Conducción del Batallón de Comunicaciones; ROP 05-05; Edición 1998; Anexo 1; artículo 1001, p. 51.

En el apoyo de los servicios de Informática y Comunicaciones en las dependencias del EMCFFAA para instalar, operar y mantener el "Sistema de Comunicaciones Particular de la Defensa" (SICODE) en apoyo al IM, a fin de facilitar el trabajo específico del Organismo.

Intervenir en:

- La Organización, Dirección y Control de los Cursos de capacitación y perfeccionamiento Conjunto y Combinado referidas a Comunicaciones, Informática y de Guerra Electrónica.

- Todos los programas informáticos que se desarrollen en el ámbito de la Defensa que tengan aplicación en forma parcial o total que faciliten la conducción del EMCFFAA y otros organismos que utilicen la Red de la Defensa a través del SICODE[19].

6. Organización de la Jef VI – C3 I GE:

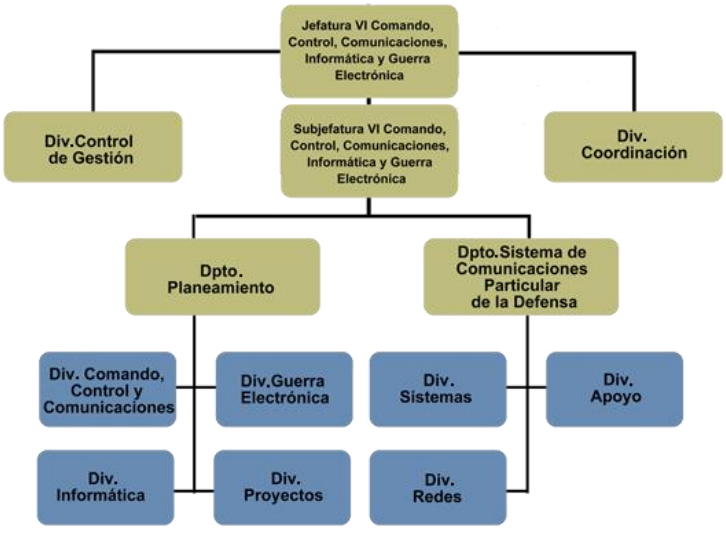

Gráfico Nro: 3 Organización de la Jefatura VI – C3 I GE[20].

[19] Estado Mayor Conjunto de las Fuerzas Armadas. Recuperado de *http://www.fuerzas-armadas.mil.ar/JVI.aspx*

[20] Estado Mayor Conjunto de las Fuerzas Armadas. Recuperado de *http://www.fuerzas-armadas.mil.ar/JVI.aspx.*

CONCLUSIONES PARCIALES

En este segundo capítulo se ha querido dejar a consideración, tomando como base el trabajo realizado por el General de División (R) Benjamín Michavila Pallarés – (España), "Los Sistemas de Comando (C4I) y la Defensa" y lo desarrollado por la Dirección General de Comunicaciones e Informática – (Argentina), en la implantación de principios que requieren una serie de medidas, entre las cuales podemos mencionar: la creación de una organización o elemento de comunicaciones con autoridad responsable sobre la seguridad a nivel operacional. Así también, obtener las herramientas necesarias; fijar los conocimientos y adiestramiento del personal de ese elemento; implementar y desarrollar nuevas herramientas de seguridad informática y promulgar las normas y procedimientos más apropiados a la realidad del campo de combate moderno en el nivel operacional, basándonos en conceptos rectores fijados por la doctrina argentina para el establecimiento de los subsistemas de telecomunicaciones particulares en los distintos niveles de la conducción.

Podemos inferir, que estos cambios, impondrán una constante capacitación del personal destinado a este órgano operativo en lo relacionado con nuevas tecnologías, como así también una constante actualización de los medios materiales y equipos, como queda expresado en el perfil del perito informático, establecido en el proyecto de la Dirección General de Comunicaciones e Informática, para poder asegurar una mejor, o como mínimo una capacidad igual al de los posibles oponentes considerados, a fin de brindar / obtener la información necesaria para la toma de decisiones.

En resumen, los avances tecnológicos en la teleinformática impondrán una oportuna y continua modificación de nuestros cuadros de organización y por consiguiente capacitación del personal del arma de comunicaciones a fin de cumplir con las exigencias que el campo de batalla moderno impone en el nivel operacional.

CAPÍTULO 3

"PROPUESTA DE ESTRUCTURA Y ORGANIZACIÓN DE LA COMPAÑÍA DE SEGURIDAD INFORMÁTICA EN EL NIVEL OPERACIONAL".

1. Finalidad del capítulo

Proponer las características más adecuadas para identificar la necesidad de ajustes en la organización y funcionamiento de un elemento de comunicaciones destinado a brindar la seguridad informática en el nivel operacional.

SECCIÓN 1

PROPUESTA DE CAPACIDADES DE LA COMPAÑÍA DE SEGURIDAD INFORMÁTICA PARA LA ACCIÓN MILITAR CONJUNTA

En el desarrollo de la presente sección se brindamos los lineamientos para establecer las capacidades y conocimientos técnicos distintivos de este elemento de comunicaciones tan particular y de la relevancia que adquiere la permanente capacitación de sus integrantes.

A continuación se brindan algunas de las capacidades que debe cumplir este elemento de seguridad informática. Es necesario destacar que este proyecto desarrollado por la Dirección de Comunicaciones e Informática del Ejército Argentino es una propuesta más y está siendo evaluada su aplicación en un período próximo que anexado al trabajo presentado busca materializar las necesidades de seguridad informática en el nivel operacional, partiendo de la base de necesidades específicas a cubrir en el manejo de la información.

- **Con capacitación o capacidad de:**

  - Expertos en sistemas operativos, los tres fundamentales: Unix y/o derivados, Windows, y OS X.
  - Conocer las vulnerabilidades de estos sistemas que aparecen a diario y desarrollarán herramientas para aprovechar esa ventaja.

- Investigar la última información disponible sobre la seguridad de estos sistemas.
- Evaluar y practicar técnicas de ataque a esos sistemas con la finalidad de detectar vulnerabilidades en los propios sistemas y en el software utilizado.
- Ejecutar operaciones defensivas, con la finalidad de proteger nuestra información y los sistemas de información.
- Ejecutar auditorias de seguridad.
- Utilizar aplicaciones disponibles en la actualidad para auditar la seguridad de redes y sistemas de información.
- Crear y hacer cumplir las directivas de seguridad informática.

- **Respuesta a Emergencias**

- Conformar un equipo para responder a emergencias y catástrofes.
- Empleo de Antivirus, backups, y directivas de recuperación de desastres.

- **Cripto**

- Desarrollar algoritmos criptográficos.
- Analizar códigos encriptados (criptoanálisis).
- Desarrollar / ejecutar directivas criptográficas.

- **Legal**

- Investigar todo lo relacionado a temas legales en las actividades de Guerra Informática.
- Amparar legalmente las actividades del elemento de Operaciones Informáticas.

- **Bases de Datos**

- Realizar el monitoreo del tráfico informático.
- Mantener la información en bases de datos.
- Desarrollar aplicaciones para acceder a esa información rápidamente.

- **Ingeniería Social**

- Es el principal elemento de Operaciones Informáticas.
- Será el nexo con el sector privado y el elemento.

- Colaborará con el Oficial de Personal sobre la obtención de recursos humanos.

- **Mantenimiento**

- Será el elemento que desarrollará las actividades logísticas y administrativas.
- Asesorará sobre el abastecimiento y mantenimiento de hardware y software[21].

SECCIÓN 2

PROPUESTA DE ESTRUCTURA Y ORGANIZACIÓN DEL ELEMENTO DE COMUNICACIONES CONJUNTO DE SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN A NIVEL OPERACIONAL

En la sección anterior, de acuerdo a lo que establece la doctrina vigente, la subunidad de comunicaciones de brigada, el batallón de comunicaciones y la jefatura VI - C3 I GE, poseen una capacidad limitada para brindar la seguridad informática necesaria a sus medios instalados, tanto en campaña como en guarnición y actividades administrativas, debido a los constantes avances tecnológicos y al empleo de los mismos en la afectación del comando y control del oponente, por lo que cobra vital importancia la protección de la información.

Los avances tecnológicos mencionados en las secciones y capítulos anteriores, imponen una reestructuración en la organización de los mencionados elementos, en nuestro caso particular el nivel operacional.

A continuación se presenta una posible organización del elemento de telecomunicaciones destinado a dar respuesta a esta necesidad de seguridad informática y tratar de satisfacer las exigencias que los desarrollos tecnológicos en materia de transmisión y seguridad de la información requiere.

Por lo mencionado en el párrafo anterior, surge la necesidad de crear un nuevo elemento de seguridad informática en el nivel operacional. Generar un elemento de nivel compañía, porque ya que este se ajusta a las capacidades y realidades que requiere el nivel operacional, en el ámbito de las fuerzas armadas.

[21] Ejército Argentino; Proyecto de la Dir Grl de Com e Info. 05 de Octubre de 2011. Recuperado de *www.cominf.ejercito.mil.ar*

A continuación se muestra una posible organización de la compañía de seguridad informática.

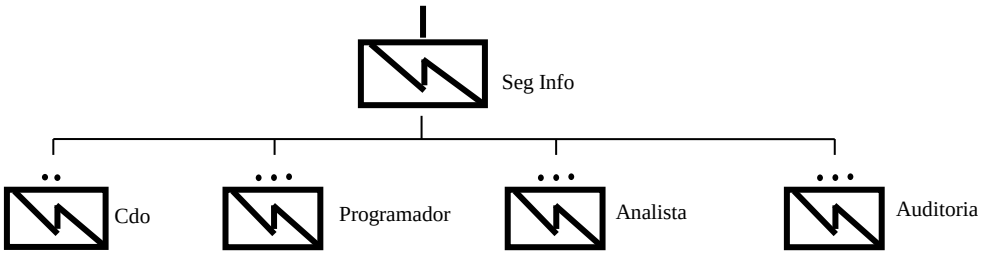

Gráfico Nro: 4 Organización de la Subunidad de Seguridad Informática[22].

CONCLUSIONES PARCIALES

El campo de combate moderno, como en las actividades guarnicionales y administrativas, impone proteger la información. Una de las posibles formas de hacer frente a las necesidades cada vez más exigentes con recursos cada vez más escasos es disponer de excelencia tanto organizativa como técnica imponiendo esto modificaciones a las organizaciones existentes en los distintos niveles de la conducción, pero sobre todo en el nivel operacional.

Los avances tecnológicos en su aplicación en el concepto Sistemas de Mando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento (C4ISR) desempeña un papel fundamental, ya que disponer de la información adecuada, en el momento adecuado y en el formato adecuado y que se diligencie en oportunidad, es esencial en el campo de batalla actual y en especial en el nivel operacional, para que ayude convenientemente en el proceso de la toma de decisión de todo Comandante.

Las capacidades técnicas y tácticas mencionadas durante el desarrollo de este capítulo, como así también las exigencias que deben cumplimentar los integrantes de este elemento de seguridad informática en cuanto al perfil requerido y en el desarrollo de las operaciones militares y en las actividades de guarnición, hace que estos avances tecnológicos impongan una modificación en la organización del elemento de telecomunicaciones destinado a brindar la seguridad en el manejo de información.

[22] Elaboración propia.

CONCLUSIONES FINALES

Conceptos emergentes en el campo de combate moderno y en actividades guarnicionales como “Guerra Informática” y los avances tecnológicos propios de nuestros tiempos, imponen modificaciones en las organizaciones destinadas al manejo de la información donde el que la posea adquiere una ventaja de suma importancia en el proceso de la toma de decisiones.

El nivel operacional en las fuerzas armadas argentinas no cuenta con un elemento destinado a priori con la finalidad de asegurar la propia información a través de las redes informáticas. Ésta ausencia hace vulnerables a los sistemas C4ISR además de afectar lograr la interoperabilidad con otros ejércitos en el ámbito regional y mundial, en el marco de desarrollo de operaciones militares de mantenimiento de las paz.

Una adecuada planificación de la política, normas y procedimientos de seguridad informática acompañada con un adecuado planeamiento para la adquisición de modernos materiales y equipos, permitirá generar la doctrina necesaria para asegurar el manejo de la información y planificar la capacitación necesaria para el personal que se desempeñe en este elemento de telecomunicaciones.

Finalmente, con esta investigación se ha tratado de brindar un elemento más de juicio para adoptar una organización de comunicaciones destinada al manejo de la información favoreciendo al comando y control en el desarrollo de operaciones militares en el nivel operacional.

BIBLIOGRAFÍA

LEYES Y DECRETOS

- República Argentina; Decreto 381/2006. Sancionada en año 2006.
- República Argentina; Ley de Defensa Nacional; Ley 23554.; Título I; Sancionada en Abril 1988.

LIBROS

- De Salas, Oscar. Introducción a la Estrategia Operacional Terrestre en el Marco Conjunto, Instituto Universitario Naval. Año 2001.

REVISTAS

- Robbins, Elizabeth L; "Las operaciones de Información con botas en el terreno: El auge del blog militar"; Manual de Informaciones; Ejército de EEUU; Octubre-Diciembre 2008.
- Sánchez Herráez, Pedro; "Guerra de cuarta generación y las redes"; Ejército de tierra español; Noviembre 2008.

REGLAMENTOS

- US Army; Communications in the Corps/Division; FM 11-30- MSE; Edition 2002.
- US Army; Signal Troposcatter Company (Light and Heavy); FM 11-25; Edition 2002.
- Ejército Argentino; Conducción de la Subunidad de Comunicaciones de Brigada; ROP-05-07; edición 1997.
- Ejército Argentino; Conducción de Comunicaciones; ROD-05-01; edición 2001.
- Ejército Argentino; FROT Nro 02/05 Sistema C4ISR digital integrado; Buenos Aires; Año 2005.

- Ejército Argentino; Centro de Comunicaciones de Campaña; ROP-05-10; edición 2007.
- Ejército Argentino; DRO Nro 01/08 Sistema Integrado de Comando y Control Táctico del Ejército Argentino "SITEA"; Buenos Aires; Año 2008.
- Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; Doctrina Básica para la Acción Militar Conjunta; PC-00-01; edición 2012.
- US Army; Field Manual Information Operation: Doctrine, Tactics, Techniques and Procedures; FM-3-13; Edition November 2003.
- US Army; Field Manual Electronic warfare; FM-3-36; Edition November 2012.

PUBLICACIONES

- Beretta Héctor, "Utilización del potencial nacional informático para el incremento del poder de combate en el nivel teatro de operaciones y superiores". Escuela Superior de Guerra, Buenos Aires; Octubre 2009.
- Prieto José, "La innovación, clave en los sistemas de mando y control de defensa", España; 2012.
- Ratti Alejandro, "La Interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control en el nivel estratégico operacional". Escuela Superior de Guerra, Buenos Aires; Octubre 2011.

REVISTAS

- Ejércitos y Batallas: Los ejércitos de tierra de la guerra del golfo de 1991. Osprey. Año 1994.
- Military Review, La Guerra del Golfo, Operación Desert Shield / Desert Storm. Edición Hispanoamericana. Enero – Febrero 1992.

PÁGINAS DE INTERNET

- Michavila Pallarés Benjamín, General de División (R) – España, **"**Los Sistemas de Comando (C4I) y la Defensa**",** Recuperado de:

http://www.afcea.org.ar/publicaciones/comando.htm. Consultada en julio de 2014.

- Estado Mayor Conjunto de las Fuerzas Armadas. Recuperado de: *http://www.fuerzas-armadas.mil.ar/JVI.aspx*. Consultada el 14 de septiembre de 2014.

- Proyecto de la Dirección General de Comunicaciones e Informática. 05 de Octubre de 2011. Recuperado de: *http://www.cominf.ejercito.mil.ar*. Consultada el 27 de agosto de 2014.