IESE
Instituto de Enseñanza Superior del Ejército
Instituto Universitario Art 77 – Ley 24.521
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL DE LICENCIATURA

Título: "INFLUENCIA DEL DESARROLLO TECNOLÓGICO EN LA ORGANIZACIÓN DEL ARMA DE COMUNICACIONES PARA LA CONDUCCIÓN DE OPERACIONES MILITARES A NIVEL TÁCTICO"

Que para acceder al título de Licenciado en Estrategia y Organización presenta el

Mayor SERGIO ALBERTO VELASCO

Director de TFL: Coronel LUIS MARIA GARRO

Ciudad Autónoma de Buenos Aires, 26 de septiembre de 2013.

ABSTRACT

Autor:	**Mayor SERGIO ALBERTO VELASCO**
Título:	**Influencia del desarrollo tecnológico en la organización del arma de comunicaciones, para la conducción de operaciones militares en el nivel táctico.**
Lugar:	**Escuela Superior de Guerra**
Oportunidad:	**Año 2013**

Problema:

La tecnología nos impone cambios, estos cambios nos proponen nuevos desafíos por lo tanto es pertinente cuestionarnos:

¿Cómo debería estructurarse el Arma de Comunicaciones para el uso y manejo de la Información en el nivel Táctico acorde al desarrollo tecnológico?

Abstract:

Este trabajo de investigación tiene por objetivo establecer cómo influyen las nuevas tecnologías desarrolladas en el Arma de Comunicaciones, tendiente a establecer necesidades o no de modificar nuestros cuadros de organización a nivel táctico.

El desarrollo del presente trabajo a realizar tiene relación con los trabajos desarrollados hasta el momento, en la Escuela Superior de Guerra, sobre los Sistemas C3I 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 necesidades de la conducción de distintos niveles y/o subsistemas componentes, para satisfacer los mencionados requerimiento.

Trataremos de dar una posible solución a este problema, para lo cual, el presente trabajo se divide en los siguientes capítulos:

Capítulo I: En el presente capítulo desarrollará el surgimiento, la evolución e implementación del C4ISR en el Ejército de Estados Unidos de Norteamérica para extraer experiencias, conclusiones y adaptarlas a nuestras necesidades, sin llegar a profundizar en detalles técnicos que harían sumamente extenso nuestro trabajo y cuya finalidad no es la perseguida.

Capítulo II: En este capítulo trataremos de determinar y analizar las características de los avances tecnológicos para identificar su impacto en el desarrollo de la estructura del arma de comunicaciones, buscando lineamientos, pautas, normas y principios que se aplican en la actualidad en otros ejércitos y en al medio civil para el diligenciamiento y registro de la información.

Capítulo III: Tomando las características de nuestros sistemas de C4ISR, a partir de tendencias de otros ejércitos, relacionados con la interoperabilidad de los sistemas, trataremos de ajustar esas experiencias y capacidades desarrolladas y ajustarlas a las necesidades de nuestra fuerza a nivel táctico.

Capítulo IV: Con la finalidad de determinar y analizar las características más adecuada para identificar la necesidad (o no) de ajustes en la organización / funcionamiento del arma de comunicaciones, buscamos una propuesta que permita cubrir las necesidades de la seguridad en nuestras comunicaciones en lo relacionado con el manejo de la información.

Mayor SERGIO ALBERTO VELASCO
ESG – COEM 2013

ÍNDICE

INTRODUCCIÓN

Influencia del desarrollo tecnológico en la organización del Arma de Comunicaciones, para la conducción de operaciones militares en el nivel táctico.

1. Antecedentes y justificación del problema.

a. Antecedentes:

El desarrollo del presente trabajo a realizar tiene relación con los trabajos desarrollados hasta el momento, en la Escuela Superior de Guerra, sobre los Sistemas C3I 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 necesidades de la conducción de distintos niveles y/o subsistemas componentes, para satisfacer los mencionados requerimiento, a continuación se detallan algunos trabajos relacionados, a saber:

- *"Acciones a llevar a cabo por el ejército argentino para optimizar la interoperabilidad desde el punto de vista combinado" del Teniente Coronel Juan Adrián CAMPITELLI - 2003*
- *Sistemas C3I en la Fuerza de Despliegue Rápido. Cap PAFUNDI y otros – Biblioteca ESG - 2003*
- *Artículo "La Interoperabilidad" del Coronel Hernán José María RISSO PATRON, del Instituto de estudios Estratégicos Buenos Aires.*
- *Interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control en el nivel estratégico operacional. My Alejandro RATTI – Biblioteca ESG - 2011*
- *La innovación, clave en los sistemas de mando y control de defensa, por José PRIETO, Director de Desarrollo de Negocio y Relaciones Institucionales – Homeland Security and Defense – GMV.*

Sin embargo, no encontramos estudios específicos del arma de comunicaciones que profundicen en la problemática del impacto de los desarrollos tecnológicos en su organización y estructura, en el desarrollo de operaciones militares de nivel Táctico.

b. Justificación del problema:

En cualquier momento de la historia que analicemos nos damos cuenta que el desarrollo tecnológico ha impuesto cambios dentro del campo de combate, indiferentemente al arma o servicio al cuál queramos hacer mención, pero la conducción de las operaciones militares siempre ha contado con un sistema de Comando, Control, Comunicaciones, Informática e Inteligencia (C4ISR) para apoyarse. Los sistemas de C4ISR anteriores al Siglo XX no han variado significativamente en su esencia y capacidades, impulsados por las necesidades de

los conductores del manejo de la información y adelantarse a lo que el enemigo pueda realizar.

Sin embargo, en estas últimas décadas con la aparición de los sistemas de comunicaciones basados en emisiones radioeléctricas y posteriormente con la informática, los alcances y capacidades de los Sistemas C4ISR emprenden una vertiginosa aceleración en su desarrollo. No solo se debe hacer mención a los sistemas de comunicaciones convencionales sino, que se ha desarrollado Sistemas de Guerra Electrónica (GE) que buscan afectar las capacidades del eslabón débil del sistema enemigo y proteger las del propio C4ISR.

De lo expuesto se desprende que nos encontramos frente a un “Sistema” y que, producto de la evolución tecnológica, impone cambios de base en la organización y estructura del Arma de Comunicaciones, es más deberíamos plantearnos si el nombre del arma debería cambiar a Telecomunicaciones, para poder abarcar todas las facilidades que nos permite manejar la tecnología de hoy en día.

Nuestro Ejército ha impulsado, a través del Centro de Desarrollo de Software del Ejército (CIDESO) y trabajando en conjunto con el Instituto de Investigación Científica y Técnica para la Defensa (CITADEF), el desarrollo de un avanzado sistema de Comando y Control, el SITEA, el cual se basa en modelos de procesamiento de datos y gestión de la información diferentes a los vigentes en nuestra doctrina. Esta innovación, impulsada desde el componente tecnológico, impacta de lleno en la organización y funcionamiento de la estructura del Arma de Comunicaciones. Hasta el momento, el SITEA continua en una fase de desarrollo y el alcance del impacto mencionado es aún incierto, lo que impone una necesaria y profunda reestructuración del arma lo antes posible para poder controlar y administrar el volumen de información que esta nueva tecnología brinda.

Paralelamente, es necesario desarrollar organizaciones que proteja nuestro sistema de información ante ataques de piratas informáticos (hackers), no contemplados en nuestra doctrina en los niveles tácticos, es decir, nuestras unidades y subunidades independientes no cuentan en su cuadro de organización (CO) de un elemento destinado a tal fin.

El presente trabajo tratará de brindar elementos de juicio y orientaciones, para una posible solución a este tema, mediante la posible reestructuración de los CO de los Elementos del Arma de Comunicaciones del Ejército Argentino.

c. **Planteo del problema.**

Los avances tecnológicos mencionados en telecomunicaciones e informática han sido el verdadero motor generador en la evolución de los Sistemas de

Comando y Control. Esto hace replantear constantemente la validez de las estructuras de las organizaciones, la doctrina vigente, hasta el proceso enseñanza-aprendizaje (formativos y de perfeccionamiento), los valores espacio-temporales para las operaciones, etc. En definitiva nos plantea nuevos desafíos que nos impone reformular nuestra forma de pensar y la forma de administrar y proteger nuestra información dentro de un campo de combate mucho más agresivo que el de tiempos pasados, donde el valor de la información es el bien más preciado para un comandante en el proceso de la toma de decisiones.

La tecnología nos impone cambios, estos cambios nos proponen nuevos desafíos por lo tanto es pertinente cuestionarnos:

¿Cómo debería estructurarse el Arma de Comunicaciones para el uso y manejo de la Información en el nivel Táctico acorde al desarrollo tecnológico?

2. Objetivos de la investigación

a. Objetivo general.

Determinar el diseño más adecuando de la estructura del Arma de Comunicaciones de una GUC para el empleo de las nuevas tecnologías y su empleo a nivel operacional.

b. Objetivos particulares.

1) Analizar las características distintivas de la conducción de operaciones tácticas con empleo del Sistemas de Comando y Control del Ejército de Estados Unidos para determinar diferencias con el modelo vigente.

2) Determinar y analizar las características de los avances tecnológicos para identificar su impacto en el desarrollo de la estructura del arma de comunicaciones.

3) Determinar y analizar las características de nuestros sistemas de C4ISR, a partir de la tendencia del ejército de Estados Unidos, relacionados con la interoperabilidad de los sistemas.

4) Determinar y analizar las características más adecuada para identificar la necesidad (o no) de ajustes en la organización / funcionamiento del arma de comunicaciones.

3. Aspectos sobresalientes del Marco Teórico

El marco teórico referencial para el presente trabajo, se sustenta básicamente en la doctrina básica en vigencia específica y conjunta en temas relacionados con los sistemas de comunicaciones:

a. La doctrina del Ejército Argentino que desarrolla aspectos vinculantes con los sistemas C3I Tácticos.

b. ROD-05-01 (Conducción de Comunicaciones).

c. RC-00-01(Doctrina Básica para la Acción Militar Conjunta).

d. ROP-05-07 Conducción de la Subunidad de Comunicaciones de Brigada. Año 1997.

e. FM 11-30 MSE Communications in the Corps/Division. US Army

Documentos:

a. Directiva 858/05 del JEMGE (Procedimientos para la obtención de nuevo equipamiento y modernización de efectos).

b. DRO Nro 01/08 (Sistema Integrado de Comando y Control Táctico del Ejército Argentino "SITEA").

4. Metodología a emplear

a. Una explicación literal sobre el método a emplear.

El trabajo se desarrollará principalmente partiendo del análisis de aspectos generales hasta el abordaje específico de la problemática planteada, contando para ello con la doctrina y bibliografía actualizada. Por lo tanto, el método seleccionado es *deductivo,* a fin de arribar con objetividad a las distintas conclusiones.

b. El diseño.

El método seleccionado para el trabajo será del tipo *explicativo* desarrollado en los diferentes capítulos afines a los objetivos específicos. Utilizando para su validación los siguientes pasos: Análisis bibliográfico, Análisis documental y Análisis lógico.

c. Un esquema gráfico metodológico.

Ver ANEXO 1.

DESARROLLO

CAPÍTULO I

Sistema Comando, Control, Comunicaciones, Informática Vigilancia y Reconocimiento (C4ISR) en EE. UU.

1. Finalidad del capítulo

En el presente capítulo desarrollará el surgimiento, la evolución e implementación del C4ISR en el Ejército de Estados Unidos de Norteamérica para extraer experiencias, conclusiones y adaptarlas a nuestras necesidades.

2. Estructura del capítulo

Sección 1

Surgimiento de los Sistemas de Comando y Control.

Para iniciar nuestro trabajo debemos referirnos y fijar algunos conceptos necesarios para relacionados con los sistemas de comando y control.

Partiendo sobre la base de que toda Nación, para poder proteger los intereses vitales y resolver cualquier conflicto va a requerir medios de seguridad y defensa organizados, entrenados y equipados desde tiempo de paz, siendo las Fuerzas Armadas (FFAA), en nuestro caso el Ejército Argentino, el instrumento principal para ello.

Esta necesidad y la experiencia en misiones de paz han impuesto operar en forma conjunta o combinada, con países amigos y aliados. Podemos inferir, por lo desarrollado, que nuestro ejército seguirá operando en zonas alejadas donde su integración a otros ejércitos impondrá contar con un sistema de comando y control a la altura y necesidades de los demás países para garantizar el éxito en las misiones a cumplir.

Para facilitar y flexibilizar el complejo y difícil ejercicio del mando y comando, los responsables disponen de personal, normas, procedimientos, material y medios, que se integran, como sistemas C4ISR, y en el más alto niveles de conducción y se los identifica como C3 para ejercer las funciones de comando, control y comunicaciones. Pero, a pesar de tantas siglas que se han ido incorporando, en esencia es un sistema comando y control (C2).

El proceso para la toma decisiones acertadas lleva consigo, además de voluntad, decisión, profesionalismo, sentido de responsabilidad y asunción del riesgo, entre otros factores de carácter personal, impone contar con un sistema de C4ISR superior o al menos igual al de los del adversario, en cuanto a calidad y cantidad para lograr, en lo

posible, conocer sus intenciones y proteger las nuestras, y facilitarle al comandante todos los elementos de juicio necesarios para que este se resuelva.

Pero este sistema no sólo debemos limitarlo a tiempos de guerra, por lo cual, es necesario que nuestras Unidades, Subunidades independientes y otros organismos, cuenten con estos sistemas también en guarnición, en forma estructurada y organizada, donde el mando se ejerce jerárquicamente, el flujo de información, el proceso necesario para preparar las decisiones y la transmisión de las órdenes para hacerlas cumplir, con rapidez y eficacia, supone volúmenes de datos elevados que requieren velocidad en el procesamiento y diligenciamiento.

Dotar a nuestro Ejército con sistemas C4ISR apropiados, además de preparar el personal calificado, equipado, e instruido en el marco específico, es necesario también hacerlo en operaciones conjuntas y combinadas. Es por ello necesario contar con un adecuado y sistemático programa de planeamiento para la adquisición de nuevos tecnologías, debido a que la información se ha convertido en un elemento principal de la guerra moderna.

Sección 2

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

Debido a los constantes ataques de grupos de piratas informáticos que actúan, de acuerdo a fuentes norteamericanas de seguridad informática, con el objetivo de robar información militar, económica y tecnológica y en otros campos variados como química y telecomunicaciones, El Departamento de Defensa de los Estados Unidos de Norteamérica, consciente de que esta revolución de las redes sociales 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"*[1], 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 y asigna responsabilidades por el responsable y efectivo uso de las redes sociales.

El Departamento de Ejército, con fecha del 01 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.*

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

- *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.":*[2]

- *Ser reciente y actualizada. Post no debe ser mayor de un mes.*

- *Cumplir con las directrices de operaciones de seguridad. 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."*[3]

Además, este documento expresa que la Oficina de Asuntos Públicos puede denegar la aprobación de la página si no cumple con algunas de estas cláusulas, y también brinda una página del Departamento de Defensa con instructivos para la confección y administración correcta de los sitios en cuestión.

Se analizarán las partes de este manual, que es la columna vertebral de las regulaciones que una potencia mundial ejerce sobre sus soldados y familias en la preservación de la seguridad y el manejo de la información que se cursa en las redes sociales.

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

[2] *Http://www.ourmilitary.mil/user_agreement.shtml*

[3] 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.

Sección 3

Lista de chequeo para la seguridad de las operaciones.

En la presente sección se enumeran los aspectos a considerar 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.*
- *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."*[4]

Sección 4

Implementación de las nuevas tecnologías informáticas en Ciber Ejercicios.

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 la redes sociales para mejor la respuesta social ante las grandes catástrofes como pueden ser ataque 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. Quien detecte este comportamiento podrá publicar esta información en la red

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

social y toda la comunidad automáticamente estará en sobre aviso y conociendo la novedad, sin mediar intermediarios que dilaten o transgiverce la información.

Estos ejercicios que se realizan anualmente se encuentran a cargo de la "*Agencia Federal para el Manejo de Emergencias, el Departamento de Seguridad Nacional (DHS), el Departamento de Defensa, varios gobiernos estatales y locales y muchos otros*"[5]

Los mismos se realizan a nivel nacional y tienen como finalidad "*mejorar la respuesta nacional a las grandes catástrofes, como terremotos, ataques terroristas e incidentes nucleares*"[6]

En el desarrollo y ejecución de este ejercicio se podrán comprobar el funcionamiento de las redes sociales en conjunción con las comunicaciones públicas en dos momentos fundamentales en las catástrofes o emergencias sanitarias, el antes y el después *"El cuarto ejercicio será ver cómo el gobierno federal y los estados pueden abordar el tema de las comunicaciones públicas, cómo el público va a ser notificado de un evento cibernético, ¿qué tipo de tecnologías se utilizarán para mantener informado al público", dice Michael Chumer, profesor de investigación con el Instituto Tecnológico de New Jersey. "Todo esto se unen en estos momentos. No sé a qué nivel o el alcance que van a hacerlo, pero van a estar mirando a las implicaciones de los medios sociales como un potencial predictor de lo que puede estar pasando"*[7]

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

"Los medios sociales pueden ser útiles para predecir y reaccionar a una amplia gama de catástrofes, incluidos los ataques terroristas, desastres naturales y los brotes de enfermedades.

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 desastres, 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"[8].

Hasta ahora, 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, pero actualmente se está comenzando a valorar las redes sociales en su potencial en la predicción de determinados eventos, lo que contribuirá en la

5 George I. Seffers, SIGNAL Online Exclusive, December 19, 2011. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2830&zoneid=334. 03/Ago/2012.
6 George I. Seffers, SIGNAL Online Exclusive, December 19, 2011. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2830&zoneid=334. 03/Ago/2012.
7 IBIDEM.
8 IBIDEM.

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), que opera tanto en tiempos de paz como de guerra, se materializa sobre un conjunto de capacidades 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 y facilidades de comunicaciones incluyen 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, el mismo permite potenciar la acción conjunta y a interacción y enlace con los niveles decisores superiores, buscando además el acceso redundante e ininterrumpido a la información por parte de este.[9]

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 harware).*

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".* [10]

Al analizar el uso de las Redes Sociales en el mundo para determinar su influencia en las actividades Militares se pueden extraer las siguientes conclusiones:

[9] Joint Publication 6 – 0 Joint Comunications Systems. Chapter II. Pag 40
[10] IBIDEM Pag 7

Durante las operaciones de combate secretas, la experiencia del ejército de Estados Unidos nos indican que, la utilización de las redes sociales han sido unas de las causas para poner en peligro la operación o develarla, lo más importante a tener en cuenta en base a este análisis es que no solamente esta información puede ser causada por el personal que se encuentra directamente involucrado en la operación, sino 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, según lo describe Minztberg en su Libro estructura de las organizaciones.

Las redes sociales y redes de área local de las unidades desplegadas en combate han sido de mucha ayuda a las actividades de combate, facilitando en intercambio de noticias desde la óptica del soldado en primera persona y mantener a las familias en contacto intercambiando información de segura y en tiempo acorde a nuestros tiempos.

En las actividades guarnicionales, las redes sociales han demostrado ser sumamente útiles en el manejo de la información cotidiana, en el diligenciamiento de documentos 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 y durante las crisis comunicacionales publicar confiable y exacta información, siendo las transgresiones a las medidas de seguridad en la publicación de información, un aspecto a considerar permanentemente por los comandos, mediante la educación del personal y luego apelar 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.

Actualmente las redes sociales 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 ataques terroristas, desastres naturales y brotes de enfermedades, tendiendo a integrarlas a las redes relacionadas con cuestiones de Defensa Nacional.

La necesidad de comunicarse de la sociedad hace que las redes sociales sean cada vez más utilizadas. Consciente de esta necesidad el Ejército Argentino ha desarrollado sitios oficiales para lograr interactuar con los integrantes de la sociedad, buscando fortalecer la comunicación institucional y la interacción del grupo familiar con sus seres queridos en cualquier parte donde se encuentre prestando servicio.

Además de hacer conocer las actividades que se desarrollan en el ámbito específico, en el marco regional y en el marco mundial a través de la participación como integrantes de misiones de paz, muchas de estas actividades desconocidas por gran parte de la población, por otro lado, nos permite brindar la información necesaria para aumentar las fuentes de reclutamiento, llegando a lugares que antes sin la explotación de esta facilidad no se conocían.

Asimismo, nuestros soldados forman parte de la sociedad, poseyendo las mismas necesidades, y por lo tanto debemos aprovechar al máximo sus beneficios y educar al personal militar y su entorno, acerca de las transgresiones a las medidas de seguridad a

ser contempladas en las distintas situaciones que se puedan presentar tanto en operaciones como en actividades guarnicionales.

CONCLUSIONES PARCIALES

El Ejército de los Estados Unidos de América a través de la incorporación de las nuevas tecnologías y haber adoptado una serie de Contramedidas inteligencia a logrado disminuir el riesgo de la fuga de información en las redes sociales, asumiendo que la necesidad de los individuos en relacionarse con sus pares, es natural, esta comunicación la ejecutará acompañado por los adelantos tecnológicos que su época imponga.

Su concreción es de fundamental importancia debido a los roles que desempeñan nuestros hombres de armas y al riesgo que estas fugas de información representan en el campo de acción, anexados a los intentos del enemigo para obtenerla.

Por otro lado al analizar lo que ocurre con las redes sociales en el Ejército más desarrollado del mundo para orientar nuestro estudio y ver si es factible su aplicación en nuestro propio sistema de comando y control en base a sus experiencias comprobadas, podemos inferir que la utilización 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 solo la conducción de operaciones militares a través del asesoramiento para la toma de decisiones en el campo de combate, materializadas a través de la cadena de comando, sino que también en lo que respecta a las necesidades básicas del ser humano de comunicarse.

Para lograr la compatibilidad de un moderno sistema C4ISR, y la necesidad de comunicación social a través de las distintas redes desplegadas, es necesario lograr la crear conciencia de las medidas de contra inteligencia en nuestro personal a través de cursos de capacitación, debido a que no podemos afirmar que por más sistemas de vigilancia y control de nuestras comunicaciones sean altamente desarrollados en hombre termina siendo habitualmente el eslabón más débil de la cadena.

El presente capítulo nos ha brindado las siguientes conclusiones:

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

2) Concientizar a todo el personal sobre medidas de contra inteligencia relacionadas con la protección de datos grupales y personales.

3) Crear un grupo responsable para actualizar datos y contenidos de páginas oficiales en las redes sociales.

4) Individualmente se debe ser cuidadoso de no aceptar en la red social a personas desconocidas.

5) Realizar controles sobre las publicaciones de los integrantes de la Unidad / Subunidad, a fin de detectar transgresiones a las medidas de seguridad de contrainteligencia.

6) Reflejar la importancia que esta cuestión tiene para el Ministerio de Defensa de los Estados Unidos, debido a que en el 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 el de Fuerzas Armadas de otros países, que permitan la interacción concurrente con el sistema de defensa de la nación.[11]

Podemos observar, que en el Ejército de los Estados Unidos, mediante claros procedimientos y normas de empleo de los distintos sistemas informáticos en el uso de sus redes operacionales y guarnicionales, el usuario conoce sus libertades y limitaciones en el uso de las mismas en las distintas situaciones.

CAPÍTULO II

Influencia de las nuevas tecnologías en la seguridad informática.

1. Finalidad del capítulo

En este capítulo trataremos de determinar y analizar las características de los avances tecnológicos para identificar su impacto en el desarrollo de la estructura del arma de comunicaciones.

1. Estructura del capítulo

Sección 1

Experiencias y aplicaciones de la Seguridad Informática.

La tendencia a la reducción de las fuerzas armadas de todo el mundo, impone nuevos desafíos relacionados con su capacidad para superar las exigencias que impone el campo de combate moderno con la misma o con superior capacidad de combate, por lo mencionado precedentemente tomaremos algunos ejemplos del ejército de los Estados Unidos y del artículo del Director de Desarrollo de Negocio y Relaciones Institucionales, Homeland security and Defense José Prieto, relacionados con el tema.

En su Artículo “La innovación, clave en los sistemas de mando y control de Defensa”, el autor hace referencia a como el campo de combate moderno a impuesto mayor rapidez en las operaciones, eficiencia y capacidad de respuesta ante situaciones críticas, por lo que adquiere un notable impulso el desarrollo de nuevas tecnologías

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

como así también la protección de la información que de ella emana en los distintos niveles.

"*Establece que la forma más adecuada para hacer frente a estas exigencias es con nuevas tecnologías. Aquí es donde el concepto C4ISR (que engloba sistemas de Mando, Control, Comunicaciones, Informática, Inteligencia, Vigilancia y Reconocimiento) desempeña un papel fundamental, ya que disponer de la información adecuada, en el momento adecuado y en el formato adecuado y que se transmite a los destinatarios adecuados, es esencial en el campo de batalla actual para que ayude convenientemente en el proceso de decisión. Las capacidades C4ISR ofrecen mejoras en gran número de aspectos en las operaciones militares, como la conciencia situacional en todos los niveles del mando militar (información sobre el emplazamiento y el estado de las fuerza enemigas y amigas), comunicaciones tácticas, logística, personal, identificación y adquisición de objetivos, inteligencia, etc"*.[12]

El C4ISR se ha convertido en los últimos años en una de las piedras angulares del campo de batalla moderno por su efecto como multiplicador de la fuerza que asegura una cooperación eficiente entre las tres Fuerzas Armadas (ejército, fuerza aérea, marina), incluso de nacionalidades diferentes, optimizando el uso de recursos militares.

Su objetivo es obtener y mantener lo que se conoce por superioridad en la información, esto es, la ventaja relativa de un oponente sobre otro en el mando y el control de su fuerza. "*La superioridad o el dominio de la información se consigue mediante la formación de líderes para la toma de decisiones rápidas y acertadas utilizando los medios superiores de información técnica que se les proporcionan, y también mediante los esfuerzos para debilitar y negar esas mismas capacidades en el oponente, protegiendo la capacidad propia*"[13]. Llegados a este punto debe advertirse que el valor de la información, puede generar la diferencia entre un ciclo de toma de decisiones más acertado reduciendo la incertidumbre y acotando riesgos, y es aquí donde los sistemas C4ISR adquieren toda su razón de ser.

Tradicionalmente, las capacidades C4ISR dependían de métodos inadecuados para la adquisición, la gestión y la difusión de información relativa al campo de batalla (por ejemplo, la entrega manual de órdenes a los jefes de campo, una fuerte dependencia del contacto por telefonía, informes en soporte de papel y a mano, etc.).

Durante la última década, el incremento del ritmo operativo ha venido forzando a los responsables militares de la toma de decisiones a recurrir a soluciones particulares y de último momento —y, por tanto, provisionales— para los problemas relacionados con las necesidades de C4ISR.

---

[12] La innovación, clave en los sistemas de mando y control de Defensa. Por José Prieto – Director de Desarrollo de Negocio y Relaciones Institucionales - Homeland Security and Defense – GMV.

[13] IBIDEM.

Ante la falta de la solución global deseada, el camino seguido hasta el momento para unificar de alguna manera los diversos sistemas heterogéneos ha sido la producción de interfaces para que los sistemas heredados, de naturaleza y origen diversos, puedan hablar entre sí. Así pues, los esfuerzos que actualmente se realizan en el área de C4ISR están dirigidos a proporcionar una solución fiable y homogénea para la mejora de las capacidades operativas, haciendo uso intensivo de los recursos que ofrecen hoy las tecnologías de la información, con un control eficiente de los costes.

No obstante, en los últimos años, y reproduciendo la evolución tecnológica experimentada en el sector civil, los sistemas militares están avanzando hacia redes federadas interconectadas en las que diferentes grupos de servicios se exportan a los usuarios de acuerdo con el concepto de Arquitectura Orientada al Servicios (SoA). De este modo, conectando adecuadamente los diferentes sistemas de comando y control, se hace posible recurrir a la funcionalidad del sistema más apropiado en cada escenario.

"El objetivo final es que las fuerzas militares puedan estar interconectadas desde el sensor hasta el tirador, y viceversa, siguiendo el paradigma de Network Enabled Capability (NEC). Esta capacidad es fundamental para asegurar el debido compromiso de las fuerzas militares en respuesta a todo el espectro de misiones previstas para el futuro (desde las misiones de paz y otras operaciones no bélicas a la confrontación asimétrica). La finalidad de NEC es vincular sensores, responsables de la toma de decisiones, los sistemas de armas y la capacidad de apoyo para conseguir un efecto militar superior mediante un mejor aprovechamiento de la información disponible".[14]

Las redes de capacidad activada, como se ha indicado líneas más arriba, puede generar un volumen inimaginable de información. La consecuencia inmediata de disponer de un número considerable de sistemas y plataformas heterogéneos que ofrecen información sobre el campo de combate o de batalla, es la tendencia a la saturación informativa que, en muchos casos, vuelve prácticamente inútil todo el sistema. "*La superioridad en la información es, sin duda, uno de los factores fundamentales en el campo de batalla actual, pero también es importante que esta información se facilite según el mecanismo denominado Common Relevant Operational Picture (CROP). Como algunos dicen, si necesitas más de dos clics para obtener la información, estás perdiendo tiempo"*[15]. Solo con un diseño cuidadoso y en continua implicación con los usuarios finales se puede cumplir este objetivo satisfactoriamente.

Interoperabilidad es, sin duda, una de las palabras clave y de mayor importancia en cualquier debate que hoy se entable sobre el desarrollo de los sistemas informáticos militares. Se refiere tanto a la interoperabilidad operativa (la que implica a personas, procedimientos, pruebas, certificaciones, formación, etc.) como a la interoperabilidad

[14] La innovación, clave en los sistemas de mando y control de Defensa. Por José Prieto – Director de Desarrollo de Negocio y Relaciones Institucionales - Homeland Security and Defense – GMV. IBIDEM
[15] IBIDEM

técnica. Esta última es definida por el Departamento de Defensa Norteamericano como *"…La condición alcanzada entre sistemas y equipos electrónicos y de comunicaciones cuando se pueden intercambiar información o servicios de forma directa y satisfactoria entre ellos o sus usuarios …"*. La experiencia de los últimos años ha demostrado que la interoperabilidad técnica (esencial para conseguir la operativa) es un concepto complejo difícil de conseguir. Los servicios exportados hacia y desde la red antes mencionada deben poder compartir datos de una forma puntual y fiable y deben funcionar entre entidades distintas para poder dar apoyo a misiones conjuntas ya sea en el marco regional o mundial. Para que dos sistemas C4ISR interoperen eficazmente, deben poder no sólo compartir datos, sino también garantizar que se interpretan de la misma forma (es decir, de acuerdo con definiciones estándar previamente establecidas).

Asimismo, la interoperabilidad debe conseguirse desde el mismo diseño, y no a través de modificaciones realizadas a sistemas ya existentes. Esto es especialmente difícil de conseguir en el ámbito militar, en el que, con mucha frecuencia debido a restricciones presupuestarias, los proyectos no se inician desde cero y están sujetos a una exigencia previa de integración con sistemas heredados, a menudo relativamente antiguos y no diseñados para su fácil integración con los sistemas de información actuales y futuros y que, sin embargo, son absolutamente esenciales para prestar la funcionalidad requerida.

"*Existen además otros requisitos que deben tenerse en cuenta durante la fase de diseño de los sistemas, como es el de la seguridad*"[16]. En una época en que la ciberseguridad es un asunto de especial preocupación, los elementos de interoperabilidad pueden causar en determinadas ocasiones consecuencias perjudiciales para la seguridad general de las tecnologías de la información de la comunicación del sistema y, por tanto, habrán de valorarse adecuadamente.

Actualmente, existen empresas en el mercado que han realizado una labor muy importante de innovación tecnológica, desarrollando sistemas C4ISR que permiten la integración en tiempo real de información originada en unidades diferentes (tierra, mar o aire) presentes en el campo de combate o de batalla. Estos sistemas proporcionan al mando una mejor conciencia situacional y mayores herramientas de ayuda para la toma de decisiones.

Como se ha indicado anteriormente, la interoperabilidad es mucho más fácil de decir que de hacer y estos sistemas han demostrado ser interoperables con las fuerzas de la Alianza Atlántica y (lo que no es menos importante) reduciendo los recursos necesarios en cuanto a personal y conocimientos. Estos son algunos de los diferentes sistemas que actualmente podemos encontrar en el mercado:

[16] La innovación, clave en los sistemas de mando y control de Defensa. Por José Prieto – Director de Desarrollo de Negocio y Relaciones Institucionales - Homeland Security and Defense – GMV.

"El principal objetivo del programa MAJIIC (Multi-sensor Aerospace Joint ISR Interoperability Coalition) es optimizar la utilidad de los recursos de vigilancia y reconocimiento, mediante el desarrollo y la evaluación de medios operativos y técnicos de interoperabilidad para una amplia variedad de activos ISR. MAJIIC incorpora información de SAR (Synthetic Aperture Radar), GMTI (Ground Moving Target Indicator), vídeo electroóptico, infrarrojo, en movimiento y ESM (Electronic Support Measures). MAJIIC permite compartir tanto datos sin procesar de sensores y datos derivados, como informes de explotación, para que los países, individualmente, no malgasten esfuerzos reuniendo información que ya existe en el sistema"[17].

Existen distintos tipos de sistemas que proporcionan automatización en el proceso de transferencia de información y en todo nivel como por ejemplo el Sistema de Adquisición de Información y Observación (TALOS) puede adecuarse para diferentes niveles (compañía, batallón, brigada, etc.)

El DSC2S es un sistema C4ISR para el soldado a pie (que actúe por sí solo o en una compañía, grupo o pelotón) que incorpora plataformas de armas, sensores de inteligencia, evaluación de la misión, aviso de proximidad de amenaza, guía de rutas y consecución de objetivos.

"El sistema LCC2S (Landing Craft Command and Control System) permite el control, la monitorización y la coordinación de la maniobra de aproximación a la costa de las naves de desembarco en operaciones anfibias"[18]. Los distintos sistemas mencionados proporcionan capacidades de comando y control en tiempo real y asegura la adecuada gestión de todo el flujo de información necesario para las unidades implicadas en el proceso de toma de decisiones. Durante el planeamiento, una vez definida la misión, se asigna un papel específico a cada una de las unidades, estableciendo todos los aspectos relevantes de la operación: rutas, organización de las fuerzas, suministros, comunicaciones, etc.

En resumen, en el campo de combate o en el de batalla, el que posea mejores y seguros sistemas de manejo de información obtendrá una ventaja decisiva en el proceso de toma de decisiones.

Sección 2

Las características técnicas de los modernos sistemas de comando y control.

La siguiente sección tiene por finalidad desarrollar algunos conceptos sobre sistemas de comando y control y algunos aspectos de interés a la hora de desarrollar los

[17] IBIDEM.

[18] La innovación, clave en los sistemas de mando y control de Defensa. Por José Prieto – Director de Desarrollo de Negocio y Relaciones Institucionales - Homeland Security and Defense – GMV.

conocimientos de los operarios de los modernos sistemas C4ISR. Para lo cual vamos a desarrollar un artículo realizado por Benjamín Michavila Pallarés, General de División (R) – España, **"**LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA**".**

"*Proteger los intereses vitales y resolver favorablemente cualquier conflicto de la nación requiere medios de seguridad y defensa organizados, entrenados y equipados desde tiempo de paz, siendo las Fuerzas Armadas el instrumento principal para ello. 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".* [19]

El campo de combate moderno impondrá actuar en forma conjunta, y la experiencia reciente nos 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 garantizar el éxito en las misiones es imperativo ejercer el mando con exactitud y precisión en todos los elementos y escalones, lo cual supone: tomar decisiones acertadas; hacerlas cumplir con eficacia, en el debido tiempo, al mínimo costo, y hacerlo con los medios y los recursos disponibles.

Para facilitar nuestro comando y control, en el 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 (comando, control, comunicaciones, computación e inteligencia), nuestro ejército a nivel estratégico tiene desarrollado mencionado sistema no así a nivel táctico, que a pesar de tantas siglas como se han ido incorporando, en esencia es un sistema de comando, que se debe adaptar al nivel la conducción que apoye en el desarrollo de las distintas operaciones militares.

La toma decisiones acertadas por parte de cualquier comandante lleva consigo, además de voluntad, decisión, sentido de responsabilidad y asunción del riesgo, entre otros factores de carácter personal, el conocimiento, en tiempo útil, del entorno, de los medios propios y de los del oponente, cuantificando y cualificando sus características, circunstancias y, en lo posible, conocer sus intenciones.

Nuestras unidades y organismos militares llevan a cabo sus funciones, actividades y tareas, tanto en paz como en guerra, no como elementos aislados que operan por su cuenta, sino de forma estructurada y organizada en el marco regional o mundial, donde el comando se ejerce jerárquicamente, el flujo de información, el proceso necesario para preparar las decisiones y la transmisión de las órdenes para hacerlas cumplir, con rapidez y eficacia, supone unos volúmenes de datos muy considerables que requieren enormes velocidades, tanto de proceso como de transmisión. Hay que tener en cuenta, por otra parte, que la escasez de recursos impone la economía de medios y el uso de materiales normalizados y fáciles de operar y mantener, pero sin descuidar las medidas

[19] Benjamín Michavila Pallarés, General de División (R) – España, "LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA". http://www.afcea.org.ar/publicaciones/comando.htm

de seguridad en el manejo de la información, esta se logra desarrollando y creando conciencia en el manejo de la información de todos los responsable y la constante instrucción, estableciendo normas y procedimientos.

Los sistemas de comando:

"*Los diferentes elementos y órganos de comando, operativos, logísticos y servicios de apoyo, necesarios para cumplir cualquier misión militar, forman un conjunto variado y complejo, cuyos componentes deben estar interrelacionados, de modo que cada uno de los diferentes escalones y elementos pueda disponer de la información necesaria en cada momento y a la vez enviar sus órdenes, peticiones o información a los demás. Todo ello con precisión y en tiempo útil para el desarrollo de sus cometidos".* [20]

Es una responsabilidad de nuestra arma de comunicaciones dotar al ejército con sistemas de comando apropiados, además de prepararlos con personal calificado, bien entrenado, equipado y listo para las operaciones conjuntas, es absolutamente necesario para ser persuasivos en la paz, decisivos en la guerra y preeminentes en cualquier clase de conflicto. Los distintos sistemas de comando y control deben poder integrarse de modo que produzcan el intercambio de información conveniente, funcionar con garantía de seguridad y permitir la interoperabilidad entre los puestos sean necesarios en los elementos y unidades ya sea dentro del ejército como con el resto de las Fuerzas Armadas, para que, operando con rapidez, coherencia y de forma coordinada, puedan estar siempre en ventaja sobre sus oponentes.

Los desarrollos tecnológicos utilizados en los sistemas C4I facilitan la información convenientemente procesada, con una imagen actualizada de la situación y con el panorama completo de la zona de operaciones con todos los elementos desplegados, y lo relevante es que permiten un intercambio seguro en el proceso de diligenciamiento y registro de las comunicaciones.

Además permite con ello a los respectivos jefes ordenar los esfuerzos, emplear los efectivos disponibles y aplicar los medios adecuados, con precisión, exactitud y conocimiento real del entorno y de las actuaciones e intenciones del enemigo, con el fin de reducir o neutralizar sus actuaciones y efectivos. Es decir, adelantarse al oponete en el proceso de toma de decisiones.

Las tecnologías de la información:

En este aspecto vamos a mencionar lo que expresa claramente en su artículo el General Pallarés, en relación a la tecnología de la información y cóo esta ha evolucionado y ha adquirido vital importancia en el campo de combate moderno, es expresa lo siguiente:

"La información ha sido siempre importante, especialmente en las funciones de comando y de inteligencia. En la actualidad, tal exigencia se ha convertido en cuestión

[20] IBIDEM

vital para lograr el dominio de la situación, de aquí la aplicación masiva de los avances tecnológicos, no sólo procedentes de la I+D militar, sino también del campo civil".

Las mejoras en estas ramas de la tecnología impactarán significativamente en las futuras operaciones militares, proporcionando a los responsables de tomar las decisiones la información precisa en tiempo útil y en condiciones adecuadas, siendo sus características más destacables:

- *La tecnología de la información incrementa la facultad de conocer, asignar prioridades, dirigir, comprobar y evaluar la información.*

- *La fusión de todas las fuentes de inteligencia mediante la integración de la información procedente de los sensores, plataformas, órganos de comando y centros de apoyo logístico permite realizar con más rapidez un mayor número de tareas operativas.*

- *Los adelantos en las computadoras, en los nuevos sistemas determinadores de posición de ámbito mundial y en las telecomunicaciones proporcionan la posibilidad de establecer con exactitud la situación de las fuerzas amigas y enemigas, así como recoger, procesar y distribuir información importante a un gran número de puestos.*

- *La flexibilidad de los modernos sistemas C4I consigue integrar puestos de comando, terminales de información y sensores, con rapidez y facilidad, con tal de disponer en esos puntos de un enlace por cualquier medio de comunicación.*[21]

Queda reflejado que las fuerzas que utilicen las posibilidades de este «sistema de sistemas» lograrán el dominio de la información, lo que permitirá obtener mayor eficiencia en el cumplimiento de las distintas actividades operacionales en una determinada zona de operaciones o en actividades de guarnición. Aunque esto no elimine por completo la niebla o incertidumbre de la lucha, el dominio de la información y su rápido diligenciamiento mejorará el conocimiento de la situación, reducirá el tiempo de repuesta y hará que el escenario del combate sea considerablemente predecible y amigable a nuestras intensiones o a lo planeado, para imponer nuestra propia voluntad al oponente.

La Importancia de la información:

"A lo largo de la historia, obtener, explorar y proteger la información ha sido algo crítico para el comando, control e inteligencia. La inapreciable importancia de aquélla no cambiará en el futuro. La diferencia consistirá en la facilidad de acceso, asignación de prioridades y las mejoras en velocidad, precisión y transferencia de los datos recibidos mediante los avances de la tecnología. Hoy en día, los medios de captar información son exhaustivos. Todo el espectro electrónico y visual es analizado y

[21] Benjamín Michavila Pallarés, General de División (R) – España, "LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA". http://www.afcea.org.ar/publicaciones/comando.htm

evaluado para hacer inteligencia, que debe ser diseminada hasta los escalones más bajos adaptando sus necesidades.

Es fundamental para los sistemas de comando disponer de esa masiva información, hay que encontrar un medio de transportarla, procesarla y presentarla. La respuesta a esta necesidad sólo la dan las nuevas tecnologías aplicadas a los sistemas C4I. Lograr el dominio en la batalla de la información requiere conseguir la ventaja tecnológica y de organización sobre el adversario, lo cual supone tener superioridad a la hora de obtener, procesar y diseminar el flujo ininterrumpido de información, a la vez que se deniega esa facultad al adversario, teniendo en cuenta que la guerra de información es tanto ofensiva como defensiva"[22].

En la actualidad la guerra de información ofensiva reduce, elimina o distorsiona los datos del adversario, lo que se denomina guerra de la información. Es necesario incluir métodos, tradicionales (ataques de precisión para destruir o neutralizar la capacidad de comando y control del adversario) como no tradicionales (intrusión electrónica en sus redes de información y control), para confundir o engañar al comando enemigo responsables de la toma decisiones, por ello es fundamental desarrollar en nuestro caso un elemento con capacidad de efectuar estas operaciones de intrusión electrónica en las redes de información del enemigo.

Este esfuerzo no menor para lograr y mantener la superioridad en el manejo de la información lleva consigo también el poder superar con éxito no solo los ataques enemigos sino también adoptar las medidas necesarias para proteger nuestro sistema de información. Por lo cual podemos inferir que la guerra defensiva para proteger nuestra capacidad de conducir las operaciones de información será uno de los mayores retos para el futuro, y debemos reorientar los esfuerzos en seguridad de la información de acuerdo a esta nueva exigencia del campo de combate moderno.

Las nuevas tecnologías en el manejo de la información a demostrado que es necesario incluir en nuestros cuadros de organización un elemento con la capacidad defensiva tradicional de la información y sus operaciones (medidas de seguridad física y cifrado), las acciones no tradicionales de protección antivirus y métodos innovadores para la transmisión de datos con seguridad. Esto impondrá la necesidad de montar y elaborar nuevos programas de capacitación con la finalidad e mantener protegido nuestro comando y control.

Las Características de los sistemas de comando:

"*Los nuevos sistemas de comando se están desarrollando con las tecnologías emergentes en los campos de la informática y de las comunicaciones, procedentes principalmente del sector comercial, como consecuencia de su más avanzado estado, su mayor disponibilidad y mucho menor precio. La política de defensa y la estrategia militar reconocen claramente el valor de las nuevas tecnologías aplicadas a los sistemas 4I para la mejora de la eficacia y la eficiencia y, en consecuencia, se están*

[22] IBIDEM.

llevando a cabo iniciativas para conocer su viabilidad y asimilar los nuevos medios y técnicas en los modernos sistemas operativos".[23]

En el artículo "Los sistemas de comando (C4I) y la defensa", se menciona como anualmente en los ejercicios que realizan en Estados Unidos para demostrar la validez de las nuevas tecnologías, presentadas por empresas americanas, en los sistemas de defensa. Se trata de los ya famosos ejercicios de demostración JWID (Joint Warrior Interoperability Demostration), patrocinados sucesivamente por uno de los Ejércitos americanos, 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, el cual es considerado como el sistema de comando y control más innovador y de mejores posibilidades operativas. En la creación de este sistema de protección se han utilizado herramientas comerciales, adaptadas y combinadas a nuestras necesidades para lograr tales resultados, PC comerciales y comunicaciones militares y civiles formando una red, protegiéndose la comunicación con equipos de criptografía y saltos de frecuencia.

Los constantes avances tecnológicos conlleva la rápida obsolescencia, por lo cual impone un constante compromiso en la modernización/ renovación de los sistemas y equipos, es decir, agotar al máximo los ciclos de vida o modernizar/sustituir, aplicando las nuevas tecnologías emergentes. La incorporación de nueva tecnología sirve fundamentalmente para mejorar la eficacia operativa e implica la renovación de la doctrina de empleo. Por lo consiguiente impondrá si es que se quiere conservar la superioridad tecnológica, mantener el esfuerzo de modernización y capacitación del personal y elementos que se encuentran dentro de esta organización.

Los sistemas de comando y control deben facilitar a las unidades de los Ejércitos el cumplir las misiones conjuntas y combinadas que se les asignen y operar entre sí estableciendo y cumplimentando las normas y directivas vigentes para el entendimiento, analizando las más relevantes características: la interoperabilidad, la seguridad, la confiabilidad, la flexibilidad y la actualización profesional del personal y de la organización en las nuevas tecnologías emergentes.

Interoperabilidad

Es un requisito esencial que los sistemas de comando y control deben ser interoperables en todos los niveles, para lo cual mencionaremos algunas recomendaciones:

• "*Cubrir las necesidades del jefe operativo.*

• *Designar a una persona con responsabilidad y autoridad que cruce las fronteras orgánicas y lleve a cabo su misión con eficacia.*

• *Guardar el equilibrio necesario con seguridad, disponibilidad, flexibilidad, supervivencia y funcionalidad, características también importantes.*

[23] IBIDEM

• *Asegurar la interoperabilidad en base a una buena implantación y las pruebas pertinentes.*

• *Diseñar la ingeniería con flexibilidad y al mínimo coste. Para lo cual se recomienda:*
- *Emplear productos, servicios y tecnologías comerciales disponibles en el mercado, siempre que sea posible.*
- *Emplear las normas técnicas establecidas y registrar todos los datos documentando la información para garantizar la interoperabilidad durante el ciclo de vida.*
- *Probar la interoperabilidad verdadera y realizar informes de rendimiento, en ejercicios reales o de simulación"*[24].

Seguridad

Al hablar de seguridad debemos hacer mención a los conceptos rectores del apoyo de teleinformática que define Seguridad como "*Conjunto de medidas de protección a adoptar tanto para negar al enemigo toda información de valor que pudiere ser obtenida del estudio de los sistemas propios, como la protección de personas y medios disponibles….".*[25] . Queda claro que estos sistemas de comando y control deben mantener su capacidad operativa en todo momento. Para lo cual es necesaria la capacitación del personal en lo referente al manejo de la seguridad de la información en todos los niveles de la organización.

Es necesario conocer que el ataque informático es más fácil que la defensa y que los agresores cibernéticos (normalmente jóvenes que por diversión), atacan los puntos más débiles de la defensa del adversario y cuentan con el factor sorpresa para llevarlos a cabo.

"La mejora en la seguridad de los sistemas depende de una serie de principios como los siguientes: defensa en profundidad; asegurar una degradación progresiva; lograr un compromiso entre la seguridad y los demás atributos del sistema, como la interoperabilidad, la normalización y las facilidades del usuario; reconocer las debilidades inherentes de la defensa pasiva y, por último, hacer cuantos esfuerzos sean posibles para alcanzar los mejores resultados.

Conseguir la implantación de esos principios requiere una serie de medidas, entre las que merecen destacarse: la designación de una organización con autoridad responsable sobre la seguridad; garantizar la disponibilidad de las herramientas adecuadas; el entrenamiento del personal de esas técnicas; realizar los ejercicios y evaluaciones correspondientes; establecer fuertes mecanismos de autenticación; desarrollar nuevas herramientas de seguridad y promulgar los procedimientos apropiados". [26]

---

[24] Benjamín Michavila Pallarés, General de División (R) – España, "LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA". http://www.afcea.org.ar/publicaciones/comando.htm
[25] ROD 05-01 Conducción de Comunicaciones Cap V Art 5006 Pag 59.
[26] Benjamín Michavila Pallarés, General de División (R) – España, "LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA". http://www.afcea.org.ar/publicaciones/comando.htm

Flexibilidad

"*Es la adecuada distribución de facilidades que permiten que un sistema, sin modificaciones sustanciales, pueda adaptarse rápidamente a ls variaciones operacionales que, razonablemente, puedan presentarse en combate."*[27]. Un sistema de comando y control debe ser capaz de integrar con rapidez y facilidad tantos puestos de comando, terminales de información como sean necesarios para el desarrollo de las operaciones previstas en los planeamientos específicos, conjuntos y combinados, en localidades remotas y condiciones precarias. Para ello deben tener un diseño adecuado, con capacidad suficiente y con facilidad para la integración en el sistema con tal de disponer de un enlace por cualquier medio de comunicación, favoreciendo la maniobra de las operaciones y contribuyendo al comando y control.

A fin de lograr la mayor flexibilidad, los nuevos sistemas de comando y control adoptaran normalmente un diseño de comunicaciones de tipo red, que permite la conexión de tantos puestos comando como sean necesarios, independientemente de su situación geográfica, y realiza el diligenciamiento y registro de mensajes con la máxima economía de tiempo y medios.

Cultura sobre las nuevas tecnologías:

Consideramos necesario que todo el personal y la organización debe predisponerse especialmente a la incorporación de nuevos conocimientos tecnológicos y al manejo de estas nuevas tecnologías para conseguir la máxima eficacia y eficiencia en los resultados, por lo cual se debe prever los cursos de capacitación pertinentes para cada caso particular a fin de satisfacer las necesidades operacionales derivadas de tales funciones, actividades y tareas.

Por lo cual es necesario contar con un enfoque integral en el manejo de la información para lograr determinar nuestras necesidades y lograr interactuar en el marco regional y global con países amigos o aliados en la solución de no solo problemas de conflictos armados, sino también ante catástrofes naturales o en emergencias humanitarias.

Las nuevas tecnologías como hipertextos, multimedia, internet y televisión por satélite, son conocidas como tecnologías de la información y comunicaciones (TICs), para materializar una representación gráfica de lo que entendemos como TICs, mostramos a continuación la figura 1, extraída de un sitio de internet especialista en este tipo de tecnologías.

[27] ROD 05-01 Conducción de Comunicaciones Cap V Art 5006 Pag 60.

Figura 1[28]

El manejo de estas nuevas tecnologías impondrán dificultades, con el fin de reducir estos efectos se presentan las recomendaciones siguientes:

- *"El cambio cultural requiere una clara visión de lo que supone un sistema de comando en la nueva era de la información.*
- *La dirección principal de la organización debe ser persistente, patente y profundamente comprometida para conducir ese cambio cultural.*
- *Aceptar la solución del 80 por 100 en el inicio de todo nuevo sistema es esencial para su implantación y perfeccionamiento operativo posterior.*
- *Aceptar los riesgos calculados y hacer frente a las futuras contingencias.*
- *Probar los sistemas 4I de forma cooperativa, flexible y continuada.*
- *Respecto al personal, garantizar la actualización de los conocimientos a lo largo de la carrera profesional e impulsar la creación de organismos y actividades que los puedan desarrollar de forma activa. Con ello, tanto los especialistas como el personal operativo podrán tener conocimiento, a la vez, de operaciones y tecnologías, explotando al máximo, de este modo, las nuevas posibilidades.*
- *Mantener y expandir los esfuerzos en las tecnologías de la información y en los nuevos desarrollos, buscando nuevos conceptos que mejoren la eficacia operativa y de gestión".*[29]

[28] http://jeshujjts.blogspot.com.ar/2010/06/oportunidades-de-las-tic-para-mejorar.html
[29] Benjamín Michavila Pallarés, General de División (R) – España, "LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA". http://www.afcea.org.ar/publicaciones/comando.htm

Los modernos sistema de comando y control y las nuevas tecnologías ofrecen una ventaja muy importante en el campo de combate moderno al momento de empeñar en operaciones a fuerzas militares aumentando su capacidad operativa y reduciendo la incertidumbre del combate en el artículo que durante este capítulo hemos estado mencionado se los denominó «multiplicadores de la Fuerza» (force multipliers).

Este potencial se verá aumentado en un correcto uso de los sistemas de información para obtener las vulnerabilidades en cuestiones de seguridad el enemigo a aprovecharlos al máximo para establecer los mecanismos necesarios para facilitar su afectación como así también proteger el propio. "*Solamente con las debidas acciones mantenidas en el tiempo se podrá conseguir el resultado deseable*."[30]

CONCLUSIONES PARCIALES

En este capítulo hemos querido dejar a consideración, tomando como base el trabajo "*La innovación, clave en los sistemas de mando y control de Defensa. Por José Prieto – Director de Desarrollo de Negocio y Relaciones Institucionales - Homeland Security and Defense – GMV*", en la implantación de principios necesarios que requieren una serie de medidas, entre las cuales podemos mencionar: la creación de una organización con autoridad responsable sobre la seguridad en el manejo de la información; obtener las herramientas necesarias; fijar los conocimiento y entrenamiento del personal de ese elemento; fijar los mecanismos de autenticación; implementar y desarrollar nuevas herramientas de seguridad y promulgar las normas y procedimientos más apropiados a la realidad de nuestro ejército, basándonos en nuestros conceptos rectores para el establecimiento de los subsistemas de comunicaciones particulares en los distintos niveles de la conducción.

Podemos inferir, que impondrá una constante capacitación del personal destinado a este órgano operativo, como así también, una constante actualización de los medios materiales y equipos, para poder asegurar una mejor, o como mínimo una capacidad igual al de los posibles enemigos considerados, a fin de obtener la información necesaria para la toma de decisiones.

CAPÍTULO III

Impacto de las Nuevas Tecnologías en la Seguridad Informática.

1. Finalidad del capítulo

Determinar y analizar las características de nuestros sistemas de C4ISR, a partir de la tendencia del ejército de Estados Unidos, relacionados con la interoperabilidad de los sistemas.

[30] IBIDEM

2. Estructura del capítulo

Sección 1

La aplicación del SITEA en la dirección y el control de las operaciones.

Para desarrollar el siguiente capítulo nos vamos a apoyar en la experiencia del ejército de Estados Unidos en el marco internacional, como así también en el desarrollo del Sistema Táctico del Ejército Argentino (SITEA) y en nuestra doctrina vigente, focalizándonos en lo referente a concepción y la seguridad en el manejo de la información. Para apoyar la dirección y el control de las operaciones, SITEA nos brinda herramientas muy útiles para apoyar las continuas apreciaciones de situación y facilitar la toma de decisiones a todo nivel de la conducción. No obstante, hay que mencionar que durante el desarrollo de una operación, cobran real importancia las capacidades de los restantes subsistemas y su integración en tiempo real con accesibilidad desde todos los niveles de comando (según el criterio de necesidad de saber). En la actualidad esto lo logramos parcialmente en nuestro ejército a través de la utilización de equipos radioeléctricos encriptados, pero en la transmisión de video e imagen todavía no se cuenta con un medio seguro y confiable, y nuestra doctrina del arma de comunicaciones no tiene desarrollada esta capacidad.

A continuación se mencionarán algunos componentes del SITEA, necesarios para realizar nuestro análisis de aplicación en la dirección y el control de las operaciones.

1. El software básico / la Visión Táctica Integrada:

(… "Poseer una visión táctica integrada es una preocupación de todo comandante, se asemeja a lo que los sistemas C2 extranjeros mencionan como Common Operational Picture (COP).

La idea básica, es fusionar sobre un SIG común a todo nivel:

- *La situación de los Elementos propios (ubicación y estado)*
- *La información proveniente de los sensores.*
- *La inteligencia procesada por un elemento. (Blancos, actividad del enemigo, etc).*

Asimismo, los usuarios podrán acceder a la información logística que las respectivas áreas hayan ingresado, respecto de los Elementos dependientes y del B Log de la GUC.

Se busca desarrollar en la práctica, el principal punto de vinculación de los subsistemas que SITEA intenta integrar, es decir, los sistemas de inteligencia / información y Apoyos de Fuego, Apoyo Logístico. Es la representación visual al Comandante y su Estado Mayor sobre lo que acontece en su zona de responsabilidad, plasmado en forma sintética sobre pantallas y/o terminales de computadoras.

De manera tal, quienes acceden a la visión táctica integrada, encontrarán condensada toda la información necesaria sobre el ambiente geográfico, propia tropa y el enemigo.

La finalidad de esta representación dinámica es que se pueda acceder tanto desde una posición estática como ser en el Puesto comando, o en movimiento desde el Puesto Comando Táctico"…)[31]

2. Los Puestos Comando y los sistemas comando y control para las Unidades Dependientes:

El SITEA prevé estar en capacidad para operar simultáneamente en el nivel Gran Unidad de Combate, Puesto Comando Principal, Puesto Comando de Retaguardia y un Puesto Comando Táctico.

Pero esto demandará un gran esfuerzo para dotar del material necesario a los Puesto Comandos de las Unidades / Subunidades Dependientes. A nivel Unidad, se reconoce y será una responsabilidad de los jefes de elementos, que las mismas deben disponer de su propio segmento de comando y control, lo que se conoce normalmente como *Battle Management Systems* (BMS), en el ejército de los Estados Unidos. El sistema de comando y control (C2) de las Unidades se configura alcanzando los niveles Subunidad y Sección. El software específico para este nivel aún se encuentra en etapa de estudio.

La implementación del SITEA a nivel táctico con las características propias del PC Un, se reducen en lo referido a instalaciones, por lo cual el equipamiento adecuado para soportar el sistema debe ser sumamente flexible y con capacidad de ser operado desde un vehículo y con capacidad de operación estático con el despliegue de mínimos componentes.

Las computadoras de campaña adquiridas (militarizadas / endurecidas), permiten su operación desde un escritorio convencional en una carpa conectada a la red informática, y en caso de desplazamiento, montarse sobre una base previamente fija en el vehículo y continuar conectada a la red a través del equipo de radio.

Es decir, cobrará relevancia la Interoperabilidad**,** debido a que los sistemas C2 deben poder integrarse en todos los niveles, para lo cual se pueden tomar como base algunas recomendaciones:

- *(… "Cubrir las necesidades del jefe operativo.*

- *Designar a una persona con responsabilidad y autoridad que cruce las fronteras orgánicas y lleve a cabo su misión con eficacia.*

- *Guardar el equilibrio necesario con seguridad, disponibilidad, flexibilidad, supervivencia y funcionalidad, características también importantes.*

[31] Presentación SITEA al EMCO – 07 Jun 12 (Adaptación propia).

- *Asegurar la interoperabilidad en base a una buena implementación y las pruebas pertinentes.*

- *Diseñar la ingeniería con flexibilidad y al mínimo costo. Para lo cual se recomienda:*

  -Emplear productos, servicios tecnologías comerciales disponibles en el mercado siempre que sea posible.
  -Emplear las normas técnicas establecidas y registrar todos los datos, documentando la información para garantizar la interoperabilidad durante el ciclo de vida.

- *Probar la interoperabilidad verdadera y realizar informes de rendimiento, en ejercicios reales o de simulación…)"*[32].

3. El subsistema de comunicaciones e informática:

Este subsistema es la parte medular de sistema táctico del ejército argentino y de vital importancia para nuestra arma debido al manejo de la tecnología y la información involucrada aquí, es la que materializa concretamente la posibilidad de un sistema capaz de operar todo tiempo con transmisiones múltiples y procesamiento de datos en tiempo real, es decir una responsabilidad que debe estar en capacidad de asumir nuestra arma de comunicaciones.

(… *"La Dirección de Comunicaciones e Informática, se encuentra trabajando en el diseño de un sistema de redes con distintas facilidades que permita el empleo de diversas formas de explotación, para apoyar a SITEA, tanto en situaciones estáticas como dinámicas.*

Nos encontramos en una etapa de materialización de requerimientos de SITEA, el subsistema de comunicaciones emplea equipos ya existentes en la fuerza y los complementa con nuevo equipamiento para responder a las necesidades técnicas del sistema mayor al que sirve y sostiene.

Cabe destacar que el diseño del sistema de comunicaciones e informática para SITEA continúa en etapa de evaluación y se ve condicionado por decisiones de nivel Estratégico Nacional, que definirán los límites de la tecnología a adquirir.

No obstante ello, en términos generales, se prevé equipar (al menos inicialmente) a terminales y nodos para los usuarios en cuatro niveles a saber: Comando Gran Unidad Combate, Unidad Táctica, Subunidad y Sección. Aspirando en un futuro poder avanzar sobre niveles más bajos alcanzando incluso al soldado individual, ya que es la principal fuente de información en tiempo real del sistema"…) [33] .

---

[32] La innovación, clave en los sistemas de mando y control de Defensa. Viernes 27 de enero de 2012 11:01. Por José Prieto Director de Desarrollo de Negocio y Relaciones Institucionales. Homeland Security and Defense – GMV.

[33] Presentación SITEA al EMCO – 07 Jun 12 (Adaptación propia).

De acuerdo con lo desarrollado en el párrafo anterior podemos afirmar que el Puesto Comando Principal y el Puesto Comando de Retaguardia de la Gran Unidad de Combate, dispondrá de terminales de computadoras con acceso a la red informática ya sea a través de enlaces alámbricos (cableado UPT / Fibra Óptica / HDSL) e inalámbricos dentro del área de instalación de los mismos en su zona de responsabilidad, lo que a futuro podemos inferir que necesitaremos a un grupo especializado en seguridad informática para evitar la fuga / obtención de información por parte del adversario.

Todos los nodos estarán integrados por un equipo de radio y una computadora, en cada vehículo, llegando a contar los escalones más bajos con radios portátiles Ultra Alta Frecuencia y terminales de datos tipo "tablets" para empleo desembarcado.

Como así también si integración de una red alámbrica a un sistema inalámbrico (Wi Fi), esto también podría ser reemplazado o complementado con segmentos alámbricos (HDSL o Fíbra Óptica) para la transmisión de datos en determinadas situaciones.

El mismo concepto puede ser empleado para equipar a los Puestos Comandos de la Unidad de Ingenieros y la Zona de Trenes de la GUC.

(… "El equipo de radio básico que se está analizando para adquisición, consta de las siguientes características:
Características técnicas de Harris Corporation's RF-5800H-MP FALCON® II

- *BGAN 41 Systems – INMARSAT.*
- *Sistema ALE (Automatic Link Establishment) solo para equipos HF.*
- *Transmisión de datos a tasas de 9600 bps con protocolo libre de error.*
- *GPS incorporado.*
- *Capacidad de transmisión encriptada.*
- *Contra - Contra Medidas Electrónicas digitales.*
- *Interface IP (Internet Protocol)"…)*[34].

Harris Corporation's RF-5800H-MP FALCON® I

[34] Manual del Operador Equipo Harris Corporation's RF-5800H-MP FALCON® II.

Harris Corporation's RF-5800H-MP FALCON® II

Tales capacidades permiten una confiable transmisión de voz y datos en un entorno seguro contra potenciales Contra Medidas Electrónicas (CME) del enemigo (básicamente interferencia y engaño). Para el caso de los enlaces muy alta frecuencia (VHF), la transmisión de voz y datos puede ser incluso simultánea, esta capacidad nos brinda la posibilidad de reducir el tiempo de exposición a la localización, incrementando y favoreciendo al concepto rector de seguridad sobre todo física del personal de operadores.

La disponibilidad radios con una interface IP, nos permite referirnos a "nodos", ya que posibilita no solo transmisión de datos (con o sin una computadora conectada), sino además el enrutamiento automático de los mismos a los distintos niveles del sistema, optimizando la transferencia de información al reducirse sensiblemente los tiempos de escalada en la cadena de comando. Esto supone que la información pueda ser distribuida en forma simultánea y automática a distintos usuarios, lo que supone una de sus características más importantes.

A continuación (figura 2), creemos conveniente mostrar gráficamente los distintos modelos de equipos que materializa desde un ejemplo de equipo radioeléctrico individual hasta los vehiculares, que brindan con sus capacidades anteriormente desarrolladas comunicaciones confiables y seguras dentro del campo de combate.

Figura 2[35]

[35] http://www.railce.com/cw/casc/harris/harris.htm

Asimismo, se encuentra en evaluación, la posibilidad de dotar a las Unidades Tácticas, de equipos satelitales portátiles (tipo BGAN41) para ser empleados como facilidad redundante en situaciones estáticas y su integración a nuestro Terminal Satelital de Campaña Remolcable (TSCR).

Al conectar las terminales BGAN a una computadora, se proveería de un canal de datos de banda ancha con acceso a internet e intranet y canales de voz adicionales para telefonía y permite su integración a los distintos equipos de desarrollo en la fuerza. A continuación materializamos a través de una figura un modelo de equipo BGAN a fin de mostrar el reducido tamaño del equipo y ver las múltiples facilidades y funciones que me permite explotar en el manejo de la información.

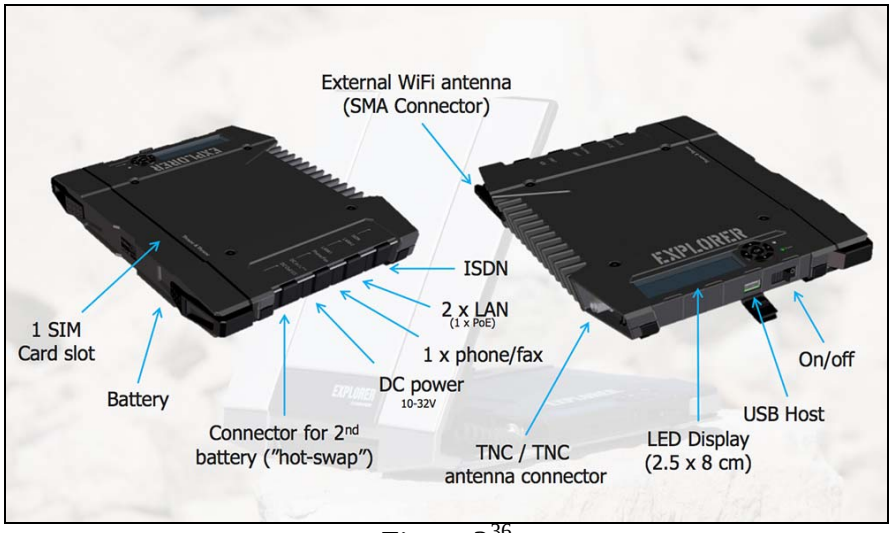


Figura 3[36]

Figura 4[37]

[36] http://www.bgan.com.mx/shop/explorer-710/
[37] IBIDEM

Sección 2

Las características técnicas del sistema y los conocimientos necesarios de los usuarios.

En esta sección se desarrollarán algunos conceptos sobre los conocimientos de los operarios de los modernos sistemas comando y control, a fin de minimizar la obtención de información por parte del oponente y que puedan afectar la conducción de las operaciones en desarrollo, como así también las actividades en guarnición.

El manejo de la guerra de la información en la guerra modera, impondrá que se disponga de personal y medios, equipados, organizados e instruidos para desarrollar actividades de protección de la propia información de las acciones del oponente, además de permitir integrarse a los sistemas de comando y control de países de la región, como así también en el marco de las naciones unidas en el cumplimiento de las diversas misiones de paz.

La historia nos enseña que la protección de la propia información, como la explotación de la información del enemigo, brindará una ventaja incalculable sobre nuestros oponentes y se transformará en un multiplicador de la fuerza.

Es necesario destacar que la infraestructura de la información del oponente (sistemas de comando y control, y las distintas redes de comunicaciones), pueden ser seleccionadas como objetivos rentables, pero no son en sí mismos el objetivo, en real objetivo es la información en sí misma que estos sistemas contienen o transportan.

a. Perfil de un Perito Informático (Conocimientos Necesarios).

En la sección anterior hemos desarrollado las tendencia evolutiva del proyecto SITEA en nuestro ejército, como así también una visión de cómo los avances tecnológicos imponen nuevas exigencias a los elementos encargados de brindar el apoyo de comunicaciones en el campo de combate moderno, a través de la visión del artículo del General Pallarés y la experiencia desarrollada por el Ejército de los Estados Unidos, y nos damos cuenta que no existe en nuestros cuadros de organización un elemento cuyos integrantes sean los responsables en temas relacionados con la seguridad y manejo de la información a través de medios de informáticos en el nivel táctico, por lo cual sería conveniente desarrollar un perfil informático necesario para realizar las tareas específicas, a fin de brindar los niveles de seguridad informática necesarios para el desarrollo de la transmisión de la información y la detección de posibles fugas de la misma, nos apoyaremos en lo propuesto en el año 2001, por la Dirección de Comunicaciones e Informática del Ejército Argentino, en lo referente al conocimiento y capacidades necesidades que debe poseer el personal que integre este elemento informático, a continuación mencionaremos el perfil necesario:

- *"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"* [38].

b. Herramientas que debe conocer y manejar el personal integrante de este elemento de trabajo:

Así como hemos hecho mención al perfil que nuestro ejército 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.
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).

[38] Proyecto de la Dir Grl de Com e Info. 05 de Octubre de 2011. Pag 8. www.cominf.ejercito.mil.ar

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" [39].

Analizando este perfil establecido como base por nuestra Dirección General de Comunicaciones e Informática, nos damos cuenta que es una necesidad que nuestra arma evolucione e introduzca en sus cuadros de organización elementos que puedan desarrollar tales funciones y tareas.[40] La Dirección General de Comunicaciones e Informática, está trabajando en la organización de un elemento operacional con la finalidad de brindar la seguridad informática a nuestra fuerza, pero hasta la fecha no ha sido materializado y más aún no se conoce desarrollo que abarque las necesidades del nivel táctico para el cumplimiento de esta misión.[41]

CONCLUSIONES PARCIALES

En este capítulo hemos querido dejar a consideración, tomando como base el trabajo realizado por Benjamín Michavila Pallarés, General de División (R) – España, "LOS SISTEMAS DE COMANDO (C4I) Y LA DEFENSA", y lo desarrollado por la Dirección General de Comunicaciones e Informática, en la implantación de principios necesarios que requieren una serie de medidas, entre las cuales podemos mencionar: la creación de un organización o elemento con autoridad responsable sobre la seguridad a nivel unidad táctica; obtener las herramientas necesarias; fijar los conocimiento y entrenamiento del personal de ese elemento; implementar y desarrollar nuevas

[39] Proyecto de la Dir Grl de Com e Info. 05 de Octubre de 2011. Pag 9. www.cominf.ejercito.mil.ar
[40] ANEXO 2 Entrevista al Jefe del Departamento de informática Coronel de Comunicaciones Sergio Onetto, destinado en la Dirección General de Comunicaciones e Informática.
[41] ANEXO 3 Entrevista al Jefe del División Desarrollo y Aplicación Capitán de Comunicaciones Daniel Orlando Bustamante, destinado en la Dirección General de Comunicaciones e Informática.

herramientas de seguridad y promulgar las normas y procedimientos más apropiados a la realidad de nuestro ejército, basándonos en nuestros conceptos rectores para el establecimiento de los subsistemas de comunicaciones particulares en el nivel de la conducción táctica.

Podemos inferir, que impondrá 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 enemigos 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.

CAPÍTULO IV

Organización y estructura del Arma de Comunicaciones a nivel táctico.

1. Finalidad del capítulo

Determinar y analizar las características más adecuada para identificar la necesidad (o no) de ajustes en la organización / funcionamiento del arma de comunicaciones.

2. Estructura del capítulo

Sección 1

Capacidades y limitaciones de la Subunidad de Comunicaciones de Brigada.

En el desarrollo del siguiente capítulo vamos a mencionar las capacidades y limitaciones con que cuenta hoy en día la Subunidad de Comunicaciones de Brigada, de acuerdo con lo que establece nuestra doctrina actual en el Ejército Argentino, como así también me voy a permitir volcar algunos conceptos propios sobre cuales a mí entender serían las capacidades que se deberían incrementar en mencionado elemento para satisfacer las exigencias de los nuevas tecnologías sobre todo en lo referente al manejo de la información a través de sistemas informáticos a nivel táctico, 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*"[42].

Podemos inferir por la definición mencionada que es necesario contar no solo con material de última generación para brindar la seguridad en nuestras comunicaciones, sino que se deberá contar con personal altamente capacitado y con un cierto perfil que le permita cumplimentar las exigencias que en nuestro caso, la seguridad informática, imponga a los integrantes de ese elemento operacional.

En la actualidad esto lo logramos parcialmente en nuestras subunidades independientes, a través de la utilización de equipos radioeléctricos encriptados, pero en la transmisión de video e imagen todavía no se cuenta con un medio seguro y confiable, y nuestra doctrina del arma de comunicaciones no tiene desarrollada esta capacidad.

A continuación, mencionaremos las capacidades que le han sido impuestas a nuestras subunidades independientes.

1. Capacidades de la Subunidad de Comunicaciones de Brigada:[43]

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

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.

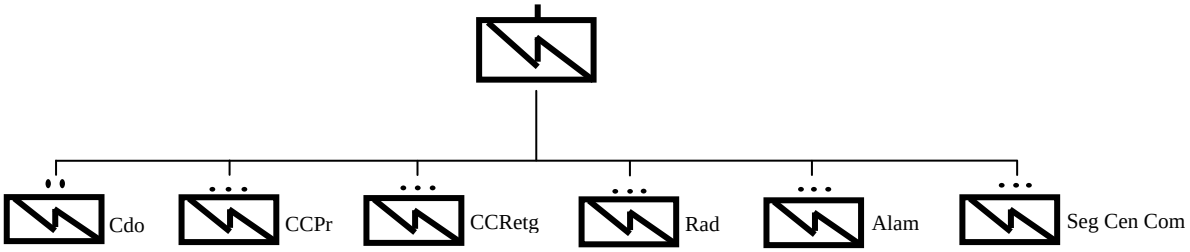
2) Dos estaciones terminales y dos estaciones repetidoras de radiomulticanal.

3) Tres redes radioeléctricas con el comando superior y dos redes radioeléctricas con los elementos dependientes.

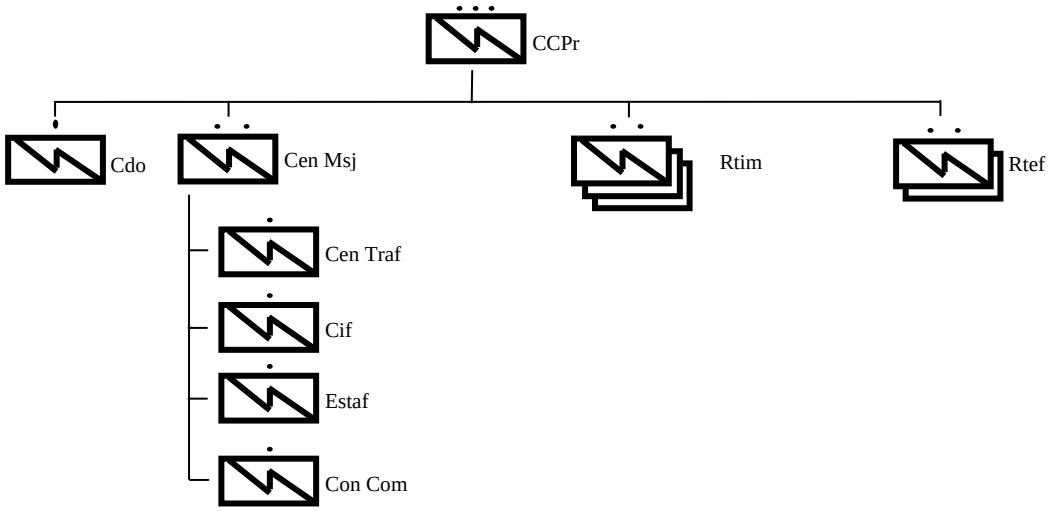
4) El sistema alámbrico del Puesto Comando Principal y del Puesto Comando de Retaguardia de la GUC y con los elementos dependientes.

[42] ROD 05 – 01 Conducción de Comunicaciones Art 3001 Pag 7. Ed 2001
[43] ROP 05-07 Conducción de la Compañía de Comunicaciones de Brigada. Art 1004 Pag 1. Ed. 1997

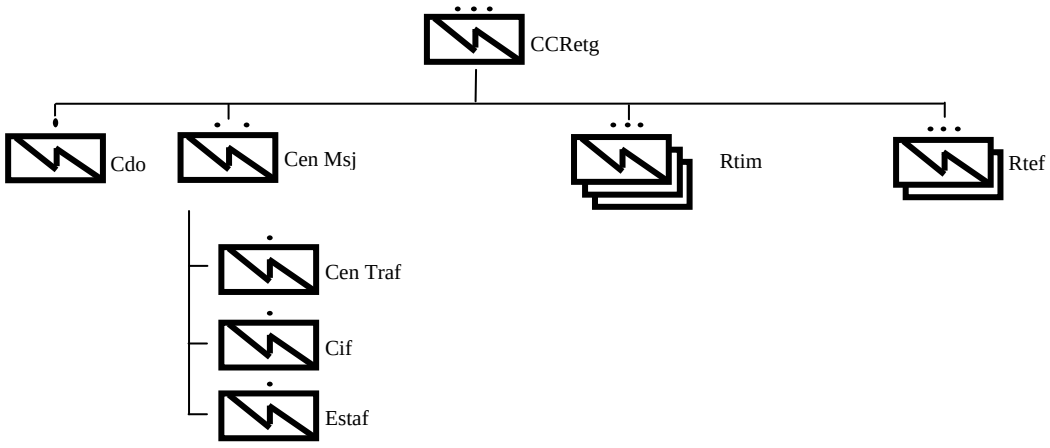
2. La Organización de la Subunidad de Comunicaciones de Brigada:[44]



3. Organización de la Sección Centro de Comunicaciones Principal:[45]



4. Organización de la Sección Centro de Comunicaciones de Retaguardia:[46]

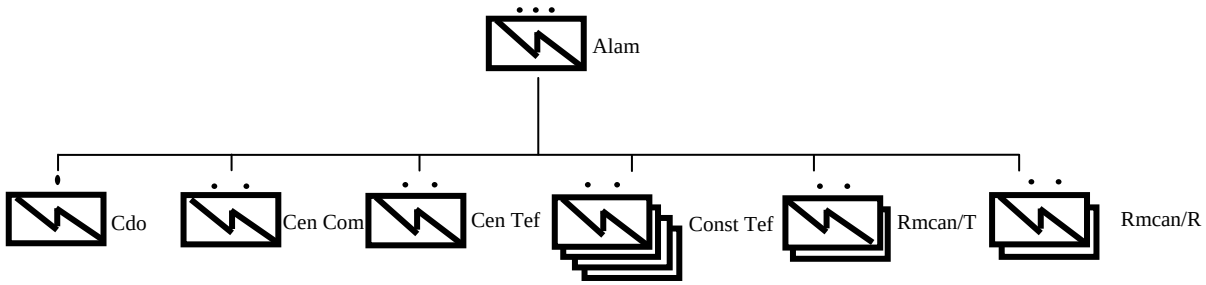


[44] ROP 05-07 Conducción de la Compañía de Comunicaciones de Brigada. Anexo 1 (Art 1001) Organización de la Subunidad de Comunicaciones Independiente. Pag 49. Ed. 1997

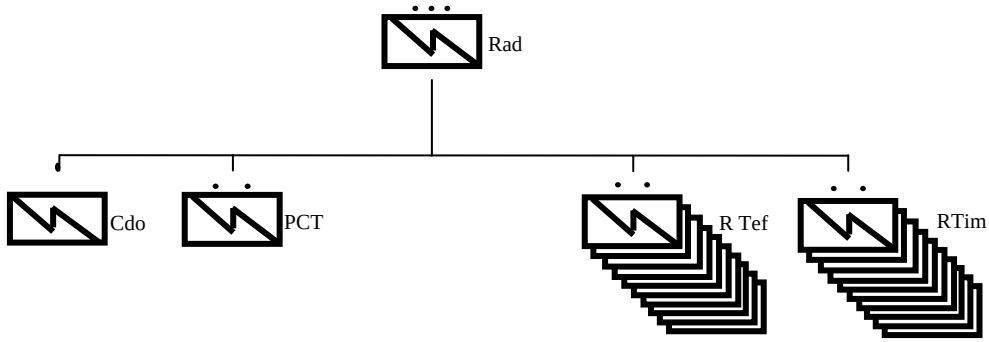
[45] ROP 05-07 Conducción de la Compañía de Comunicaciones de Brigada. Anexo 3 (Art 1025) Organización de la Subunidad de Comunicaciones Independiente. Pag 53. Ed. 1997

[46] ROP 05-07 Conducción de la Compañía de Comunicaciones de Brigada .Anexo 4 (Art 1032) Organización de la Sección Centro de Comunicaciones de Retaguardia. Pag 55. Ed. 2007

5. La Organización de la Sección Alámbrica:[47]



6. La Organización de la Sección Radio:[48]



Sección 2

Capacidades de la Sección Seguridad Informática (Propuesta)

En el proyecto que estamos haciendo mención (Proyecto de la Dir Grl de Com e Info), nos brinda los lineamientos para establecer las capacidades distintivas de este grupo tan particular y de permanente capacitación que nuestra arma debe contemplar en sus cuadros de organización. A continuación citamos las capacidades que debe cumplir esta sección de seguridad informática, es necesario destacar que este proyecto es una propuesta y está siendo evaluada su aplicación en un período próximo.

- ***"Con capacitación o capacidad de:***

  - *Expertos en sistemas operativos, los tres fundamentales: Unix y/o derivados, Windows, y OS X.*

[47] ROP 05-07 Conducción de la Compañía de Comunicaciones de Brigada Anexo 5 (Art 1037) Organización de la Sección Alámbrica. Pag 57 Ed. 2007

[48] ROP 05-07 Conducción de la Compañía de Comunicaciones de Brigada Anexo 6 (Art 1048) Organización de la Sección Radio. Pag 59. Ed. 2007

- *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 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"* [49].

Para poder cubrir las necesidades del campo de combate moderno es importante resaltar el siguiente concepto doctrinario referido a la importancia del apoyo de teleinformática:

"1.004. Importancia del apoyo de teleinformática. *El éxito de las operaciones dependerá de la conducción que el comandante pueda realizar de sus elementos dispersos, de la recepción de información, de la impartición de órdenes y de la posibilidad de satisfacer requerimientos en tiempo real.*

Será un objetivo ineludible para el éxito de la conducción preservar el propio sistema C2TI (Comando, Control, Teleinformática e Inteligencia), lo cual permitirá mantener la capacidad de mando y los mecanismos de control, a la vez que vulnerar el sistema que establezca el enemigo"[50]

Hoy en podemos afirmar que el Ejército Argentino, posee una capacidad limitada en el desarrollo de preservar en forma íntegra y completa lo establecido en el mencionado artículo, sobre todo en el último párrafo "*…a la vez que vulnerar el sistema que establezca el enemigo."*, por lo que adquiere vital importancia ante la imposición de las nuevas tecnología modificar la estructura orgánica, creando un elemento con las capacidades necesarias para cubrir estas exigencias.

Sección 3

Propuesta de estructura y organización de la Subunidad de Comunicaciones de Brigada.

Como hemos mencionado en la sección anterior, de acuerdo a lo que establece nuestra doctrina vigente la Subunidad de Comunicaciones de Brigada, ésta posee capacidad limitada para brindar la seguridad informática necesaria a sus medios instalados tanto en campaña como en guarnición, debido a los constantes avances

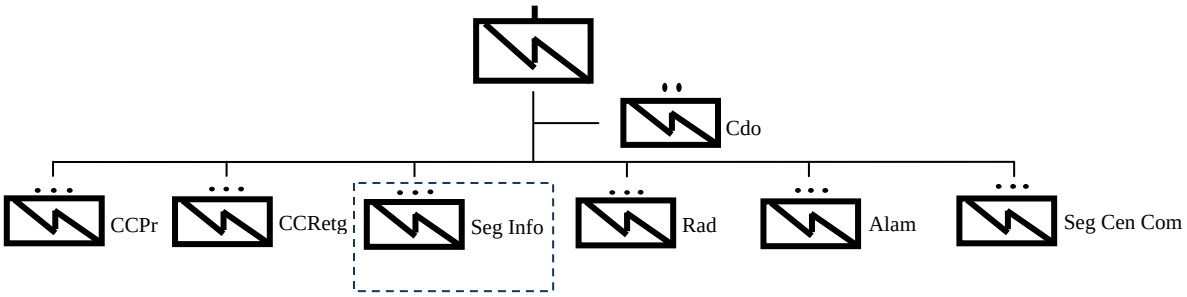
[49] Proyecto de la Dir Grl de Com e Info. 05 de Octubre de 2011. www.cominf.ejercito.mil.ar
[50] ROD 05-01 Conducción de Comunicaciones. Art 1004 Pag. 2. Ed 2001

tecnológicos y al empleo de los mismos en la afectación del comando y control del adversario, por lo que cobra vital importancia la protección de la información.

Creemos que acorde con estos avances tecnológicos mencionados en capítulos anteriores, impone una reestructuración en la organización de mencionado elemento.

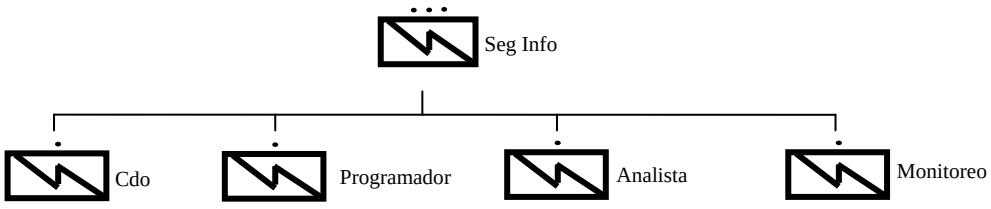
A continuación se presenta una posible modificación al cuadro de organización para dar respuesta a esta necesidad de seguridad informática y tratar de satisfacer las exigencias que los desarrollos tecnológicos en materia de transmisión y seguridad de la información requiere.

a. Por lo mencionado en el párrafo anterior surge la necesidad, a nuestro entender, de crear un nuevo elemento de nivel sección de Seguridad Informática dentro de la Subunidad de Comunicaciones Independiente.



Posible Modificación al CO

b. Propuesta de organización interna de la Sección Seguridad Informática



CONCLUSIONES PARCIALES

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, como hasta hoy nuestra arma se ha ido desenvolviendo. Los avances tecnológicos en su aplicación en el concepto C4ISR (Sistemas de Mando, Control, Comunicaciones, Informática, Inteligencia, Vigilancia y Reconocimiento) 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, para que ayude convenientemente en el proceso de la toma de decisión de todo Comandante.

Las capacidades mencionadas durante el desarrollo de este capítulo, como así también las exigencias que deben cumplimentar los integrantes de este grupo especial, en cuanto al perfil requerido, 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 comunicaciones de Brigada, para lograr cumplimentar con nuestra tarea de hacer llegar las voz del comando, donde se requiera.

CONCLUSIONES FINALES

En el presente trabajo podemos inferir que la utilización 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 solo la conducción de operaciones militares a través del asesoramiento para la toma de decisiones en el campo de combate, materializadas a través de una flexible y segura cadena de comando.

Es necesario lograr crear conciencia de las medidas de contra inteligencia en nuestro personal y generar un elemento con la capacidad de instruir y asegurar nuestra información.

A través del desarrollo de los distintos capítulos, hemos tratado de brindar conclusiones referidas al trato de la información, y su relación con actividades operacionales, ejercitaciones y fotos, que puedan comprometer la seguridad de las operaciones en desarrollo o las futuras. Además de brindar principios doctrinarios necesarios a respetar por todo el personal a fin de asegurar las medidas de contrainteligencia. Asiendo mención a la necesidad de contar con personal capacitado y un grupo responsable destinado especialmente a la protección de nuestros datos grupales y personales, a fin de evitar filtraciones de información.

Hemos tomado como ejemplo a ejércitos que han desarrollado conceptos sobre la protección de la información como el Ejército de los Estados Unidos y el Ejército de España e indirectamente al Ejército de China, que mediante procedimientos y normas de empleo de los distintos sistemas informáticos en el uso de sus redes operacionales y guarnicionales, el usuario conoce sus libertades y limitaciones en el uso de las mismas en las distintas situaciones, y que le permiten la explotación de las facilidades de telecomunicaciones en forma segura.

El avance tecnológico impone sin lugar a dudas la implantación de principios necesarios que requieren una serie de medidas, entre las cuales podemos mencionar:

a. La creación de una organización con autoridad responsable sobre la seguridad; obtener las herramientas necesarias.
b. Fijar el conocimiento y entrenamiento del personal de ese elemento.

c. Fijar los mecanismos de autenticación.

d. Implementar y desarrollar nuevas herramientas de seguridad y promulgar las normas y procedimientos más apropiados a la realidad de nuestro ejército, basándonos en nuestros conceptos rectores para el establecimiento de los subsistemas de comunicaciones particulares en los distintos niveles de la conducción.

Los avances tecnológicos en su aplicación en el concepto C4ISR (Sistemas de Mando, Control, Comunicaciones, Informática, Inteligencia, Vigilancia y Reconocimiento) desempeñan un papel fundamental, en el proceso de la toma de decisión de todo Comandante.

La interoperabilidad y las capacidades mencionadas durante el desarrollo de los distintos capítulos que contiene este trabajo, como así también las exigencias que deben cumplimentar los integrantes de este grupo especial, en cuanto al perfil requerido, 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 comunicaciones de Brigada.

Por lo mencionado con anterioridad, podemos sostener, a nuestro entender, que es necesario asignar o crear elementos con la suficiente autonomía y capacidad para asegurar nuestra información, como así también detectar aquellas amenazas provenientes de posibles oponentes en el campo virtual y en el tráfico de la información que puedan llegar a afectar el desarrollo de nuestras capacidades en el campo de combate moderno.

Para finalizar podemos inferir, que los avances tecnológicos en la teleinformática y el las telecomunicaciones, impondrán una oportuna y continua modificación de nuestros cuadros de organización y por consiguiente capacitación del personal del arma de comunicaciones, por lo cual, es necesario acompañar esta evolución para estar a la altura de las exigencias, asegurando al interoperabilidad de los sistemas con un elemento acorde a nivel táctico para lograr la eficiencia en el desarrollo de las operaciones ya sean en el marco regional y mundial.

BIBLIOGRAFÍA

Documentos:

REPÚBLICA ARGENTINA: Ley Nro 26.032 Servicio de Internet.

REPÚBLICA ARGENTINA: Ley Nro: 26.388 Delitos Informáticos.

Reglamentos:

REPÚBLICA ARGENTINA RC 00-02 Diccionario para la Acción Militar Conjunta. Ed 1999.

REPÚBLICA ARGENTINA ROD-05-01 Conducción de Comunicaciones. Ed. 2001

REPÚBLICA ARGENTINA ROP-05-07 Conducción de la Subunidad de Comunicaciones de Brigada. Ed. 1997

REPÚBLICA ARGENTINA ROP-05-05 Conducción del Batallón de Comunicaciones. Ed. 1998

Libros:

RISSOAN Romain. Las redes sociales, Facebook, Twitter LinkedIn, y Viadeo en el mundo profesional. Ediciones ENI, Libros Digitales, 2010.

Revistas:

Mayor Elizabeth L Robbins, Ejército de EEUU. Las operaciones de Información con botas en el terreno: El auge del blog militar. Manual de Informaciones Octubre-Diciembre 2008.

Pedro Sánchez Herráez Comandante Infantería DEM. Guerra de cuarta generación y las redes. Ejército de tierra español. Noviembre 2008.

Recopilación de la Redacción. La CIA habría comprado la empresa que monitorea blogs, Twitter, YouTube y Amazon. Manual de Informaciones. Julio-Septiembre 2010.

Manuales:

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

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.

Manual de redes sociales, del Ejército de los Estados Unidos de Norteamérica. Enero 2011.

Trabajos consulados:

"Acciones a llevar a cabo por el ejército argentino para optimizar la interoperabilidad desde el punto de vista combinado" del Teniente Coronel Juan Adrián CAMPITELLI – 2003.

Artículo "La Interoperabilidad" del Coronel Hernán José María RISSO PATRON, del Instituto de estudios Estratégicos Buenos Aires.

Interoperabilidad de los sistemas de comunicaciones en apoyo al comando y control en el nivel estratégico operacional. My Alejandro RATTI –Biblioteca ESG – 2011.

La innovación, clave en los sistemas de mando y control de defensa, por José PRIETO, Director de Desarrollo de Negocio y Relaciones Institucionales – Homeland Security and Defense – GMV.

Recursos electrónicos:

http://www.ejercito.mil.ar/site/home/index.asp

http://usacac.army.mil/CAC2/MilitaryReview/mrpast2.asp

http://www.infoamerica.org/articulos/textospropios/frutos/La%20necesidad%20imperiosa%20de%20comunicarnos%5B1%5D.htm. 12 de Mayo de 2012

http://www.youtube.com/watch?v=P_h5FruASHc&feature=email

http://www.comscore.com/esl/Press_Events/Press_Releases/2011/3/Social_Networking_Accounts_for_1_of_Every_4_Minutes_Spent_Online_in_Argentina_and_Chile

http://www.info7.com.mx/a/noticia/264554

http://www.20minutos.es/noticia/643188/l/facebook/soldado/israeli/

http://www.20minutos.es/noticia/372490/l/carcel/soldado/facebook/

http://news.bbc.co.uk/2/hi/8345713.stm.

http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2830&zoneid=334

http://www.wainwright.army.mil/sites/local/scr/ongoing/SocialmediaandOPSECbrief1.pdf

http://www.redes-sociales.net/

http://guerraypaz.com/2009/05/04/el-pentagono-aterriza-en-facebook-y-twitter/

http://guerraypaz.com/2011/01/16/twitter-tunez-egipto-y-el-baradei/

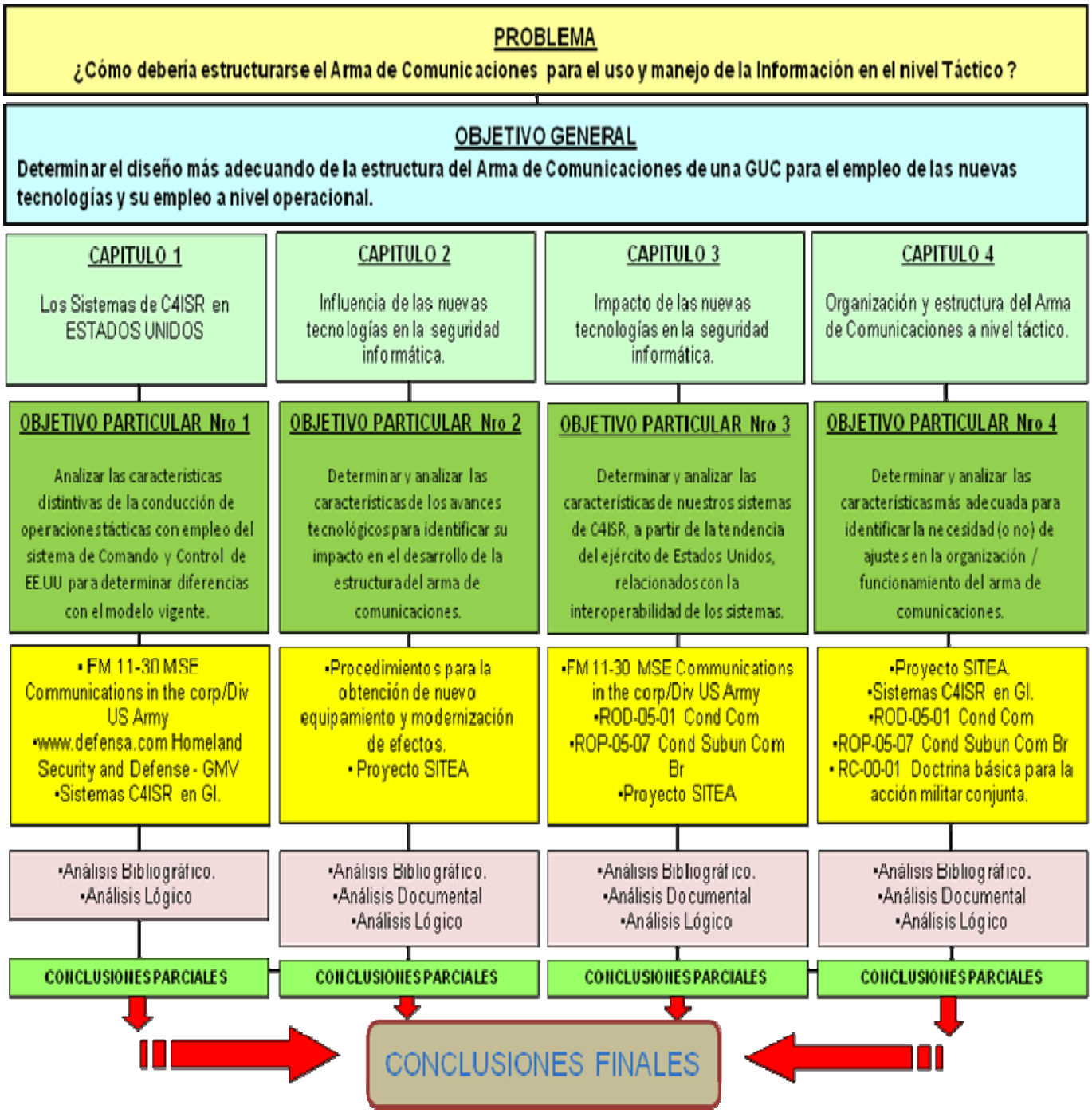
http://www.defense.gov/socialmedia/education-and-training.aspx/

http://www.globalsecurity.org/military/hotdocs.htm

http://www.guardian.co.uk/world/2011/aug/03/pentagon-monitor-social-networking-threats

ANEXOS

a. ANEXO 1 (Esquema gráfico Metodológico) AL TRABAJO FINAL DE LICENCIATURA (Influencia del desarrollo tecnológico en la organización del Arma de Comunicaciones, para la conducción de operaciones militares en el nivel Táctico).



b. ANEXO 2 (Entrevista al Coronel de Comunicaciones Sergio Onetto) AL TRABAJO FINAL DE LICENCIATURA (Influencia del desarrollo tecnológico en la organización del Arma de Comunicaciones, para la conducción de operaciones militares en el nivel Táctico).

Ejército Argentino 2013 "Año del bicentenario de la asamblea constituyente de 1813"
Escuela Superior de Guerra

Entrevista al Coronel Sergio Onetto

LUGAR: Dir Grl Com e Info
Fecha: 05 de agosto de 2013.

1. *Conforme a su experiencia en seguridad informática y como Jefe del Departamento Informática, ¿Existe a nivel ejército un proyecto referido a la creación de un elemento de seguridad informática?*

Sí, desde hace varios años la Dirección General de Comunicaciones e Informática ha estado trabajando para desarrollar el mencionado elemento, pero con la salvedad que su aplicación es a Nivel Estado Mayor Conjunto de las Fuerzas Armadas, en el cual se conforma elementos de seguridad informática. Sobre esto se han desarrollado los perfiles necesarios para cada uno de los integrantes que ocuparían cada puesto / rol.

2. *¿Considera que esos elementos de seguridad informática que usted menciona son necesarios a nivel táctico o solamente a nivel estratégico?*

Considero que deben existir a todo nivel de la conducción y ser responsables directos de la protección de la información que posean sus elementos dependientes.

3. *Relacionado con estos roles a cubrir. ¿Cuáles serían esos roles? ¿Cómo inciden en el cambio en la estructura del arma de comunicaciones como principal responsable sobre el desarrollo de esta actividad?*

Relacionado con los roles, podemos mencionar que a este nivel debería de haber un elemento de seguridad informática, otro elemento que es defensa, otro relacionado a ingeniería social (utilizado al más alto nivel de la conducción, y operado por la inteligencia militar), hay un elemento de redes, otro de mantenimiento de redes.

4. *¿Hay en el Ejército algún proyecto en desarrollo relacionado con Guerra Cibernética?*

En el ejército no hay hasta el momento un proyecto relacionado con la guerra cibernética, pero en este momento están trabajando dos comisiones, la primero está trabajando sobre un reglamento que contendría los lineamientos de empleo, pero luego yo fui destinado a otra comisión y no sé cuál es el desarrollo al día de hoy del mencionado reglamento, y fui destinado a la otra comisión destinada a la seguridad de la información, es mucho más complicado por las distintas visiones que tiene cada fuerza armada, al día de hoy estamos en un período de reorganización para seguir adelante cuando sea retomado el tema.

5. ¿Cuál es el marco legal que se está considerando para el desarrollo de este proyecto?

El marco legal en el cual se está apoyando este proyecto de seguridad informática es en una Directiva de la Oficina Nacional de Tecnología de la Informática (ONTI), adaptada a nuestras necesidades y se lo aplicó como un manual de seguridad de la información, este manual está avalado por el Director de Sistemas y cuando somos auditados por el ministerio de defensa, ellos se apegan a la regulación de lo que establece la ONTI. También en seguridad informática nos basamos en lo que establece la Directiva Nro: 823, y estamos trabajando en la actualización de esta directiva que se llamará Directiva para el Sistema Único Informático de Ejército (SUIE).

6. ¿En el ejército se está capacitando al personal para desempeñarse en estos puestos relacionados con la seguridad informática?

Lo que conozco, es que se desarrolla en la Escuela Técnica un postgrado en seguridad de la información, y en la Escuela de Comunicaciones se hacen seminarios y se capacita al personal de cursantes a través de los cursos regulares que este instituto dicta anualmente destinados a personal que tenga responsabilidades en el manejo de la información.

b. ANEXO 3 (Entrevista al Capitán Comunicaciones Daniel Orlando Bustamante) AL TRABAJO FINAL DE LICENCIATURA (Influencia del desarrollo tecnológico en la organización del Arma de Comunicaciones, para la conducción de operaciones militares en el nivel Táctico).

Ejército Argentino 2013 "Año del bicentenario de la asamblea constituyente de 1813"
Escuela Superior de Guerra

Entrevista al Capitán Daniel Orlando Bustamante

LUGAR: Dir Grl Com e Info
Fecha: 05 de agosto de 2013.

1. Conforme a su experiencia como Jefe de la División Desarrollo y Aplicación de la Dirección de Comunicaciones e Informática, ¿Conoce usted si el arma de comunicaciones está desarrollando y experimentando con algún elemento de seguridad informática?

Desconozco si el arma de comunicaciones está desarrollando y experimentando sobre seguridad informática, lo que sí conozco, es que desde hace varios años la Dirección General de Comunicaciones e Informática ha estado trabajando para desarrollar el mencionado elemento, pero con la salvedad que su aplicación es a Nivel Estado Mayor Conjunto de las Fuerzas Armadas.

2. ¿Considera que esos elementos de seguridad informática que usted menciona son necesarios a nivel táctico o solamente a nivel estratégico?

La seguridad informática abarca todos los niveles y se debe capacitar al personal para cumplir con las exigencias que esta demanda, debido a que poseer los medios más modernos no garantiza la seguridad de por sí sino que en una dupla entre material y personal para lograr proteger nuestra información de la acción del enemigo. Sobre esto se han desarrollado los perfiles necesarios para cada uno de los integrantes que ocuparían cada puesto / rol. Por lo cual, considero que deben existir a todo nivel de la conducción y ser responsables directos de la protección de la información que posean sus elementos dependientes.

3. Relacionado con estos roles a cubrir. ¿Cuáles serían esos roles? ¿Cómo inciden en el cambio en la estructura del arma de comunicaciones como principal responsable sobre el desarrollo de esta actividad?

Relacionado con los roles a cubrir, debemos contar con personal con una preparación especializada en seguridad informática y podemos mencionar que a este nivel debería de haber un elemento de seguridad informática, otro elemento que es defensa, otro relacionado a ingeniería social (utilizado al más alto nivel de la conducción, y operado por la inteligencia militar), hay un elemento de redes, otro de mantenimiento de redes, coincido plenamente con lo que ha mencionado el Jefe de la División Seguridad Informática.

4. *¿Cuál es el marco legal que se está considerando para el desarrollo de este proyecto de seguridad informática?*

El marco legal en el cual se está apoyando este proyecto de seguridad informática es en una Directiva de la Oficina Nacional de Tecnología de la Informática (ONTI), adaptada a nuestras necesidades y se lo aplicó como un manual de seguridad de la información, este manual está avalado por el Director de Sistemas y cuando somos auditados por el ministerio de defensa.

5. *Además de lo que establece la ONTI referido a seguridad en el manejo de la información. ¿El ejército argentino ha generado algún tipo de documento relacionado con el tema en cuestión?*

Sí, en el tema seguridad informática nos basamos en lo que establece la Directiva Nro: 823, y estamos trabajando en la actualización de esta directiva que se llamará Directiva para el Sistema Único Informático de Ejército (SUIE).