nales, tanto en su aspecto formal como de fondo, pudiendo atribuirse mayormente tal fenómeno a las particulares condiciones del escenario indiano.

Currículum Vitae del Cnl Hernán Federico Cornut

El Cnl Cornut integró el Cuerpo de Profesores Militares de la Escuela Superior de Guerra del Ejército Argentino, y como profesor invitado y miembro del Centro de Estudios Estratégicos en la Escuela de Comando y Estado Mayor del Ejército Brasilero. Actualmente es el Director de la Escuela de Guerra del Ejército.

Es Oficial de Estado Mayor del Ejército Argentino y del Ejército Brasilero. Licenciado en Estrategia y Organización. Posee además. El título de Magíster en Estrategia y Geopolítica y es Especialista en Conducción y Gestión Estratégica (Escuela Superior de Guerra "Tte Grl Luis María Campos").

El presente artículo tiene por finalidad dar una visión general sobre cómo los avances tecnológicos en telecomunicaciones e informática han sido el verdadero motor generador en la evolución de los Sistemas de Comando y Control.

El Sistema C3I2 en la Era de la Información

Tcnl Roberto Claudio Galizia

Introducción

El propósito de este artículo es acotar la importancia de las nuevas tecnologías, destacando su necesidad como elemento imprescindible pero no suficiente para el ejercicio del mando y control en un campo de combate mucho más agresivo, donde la revolución tecnológica nos plantea nuevos desafíos, en el cual el valor de la información es el bien más preciado para un comandante en el proceso de la toma de decisiones.

Entre los cambios más espectaculares y permanentes que ha experimentado la humanidad en su historia, podemos mencionar el del área de las comunicaciones, que ha sido producto del desarrollo de la tecnociencia contemporánea y ha revolucionado la velocidad del intercambio de información.

El constante y exponencial cambio de las nuevas tecnologías, atraviesa transversalmente a la sociedad, y produce efectos significativos en la forma de vida, el trabajo y el modo de entender el mundo por parte de los sujetos.

En el ámbito militar los avances tecnológicos 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) de los hombres de armas para la conducción de las operaciones. 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 territorialidad de un Estado presenta como componentes el espacio aéreo, na-

val y terrestre pero hoy dado los avances científicos y tecnológicos es necesario incorporar y visualizar una nueva dimensión territorial, el espacio cibernético denominado también "ciberespacio". Este espacio virtual construido por el hombre sobre la base de las infraestructuras tecnológicas de información y comunicación (alámbricas e inalámbricas) por el cual fluyen y viajan los datos y la información.

Para el Departamento de Defensa de los Estados Unidos de Norteamérica, el Ciberespacio es *"un dominio global dentro del entorno de la información que consiste en la red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados."*[1]

Asimismo, dentro de la comunidad de Tecnologías de la Información y Comunicaciones (TIC) el Ciberespacio es definido como el "*conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos"*.[2]

Esta nueva dimensión depende o está en función del creciente uso de medios, equipos electrónicos, informáticos y telemáticos por parte de las organizaciones y en general por toda la sociedad, ello supone beneficios evidentes pero también da lugar a ciertos riesgos que deben ser minimizados y controlados , a través de la aplicación de medidas proactivas y reactivas de seguridad que permitan contar con barreras defensivas y ofensivas orientadas a mitigar efectivamente diferentes tipos de amenazas y ataques.

Hoy la mayoría de las organizaciones e instituciones tienen conexión a internet, cuentan con sitios web, utilizan computadoras para diferentes procesos y algunos realizan comercio electrónico, de ahí que la tendencia es que las mismas sean cada vez más dependientes de las tecnologías de información y comunicación, lo que hace que sus infraestructuras sean críticas, siendo motivo suficiente para su resguardo y protección.

Esto ha dado lugar a la aparición de un mundo diferente, donde quizás las guerras de todo tipo no serán libradas por soldados contra soldados, sino por nuevos guerreros de la información, donde en este mundo nuevo el soldado será capaz de plantar un virus [3] en cualquier red" [4].

Sin lugar a dudas, el proceso de adaptación a dichos cambios no ocurre sin dificultades, y las instituciones militares no están ajenas a ello.

1 Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms.
2 Fojón, Enrique y Sanz, Ángel. "Ciberseguridad en España: una propuesta para su gestión", Análisis del Real Instituto Elcano, ARI Nº 101/2010
3 Virus informático: programa que tiene por objeto alterar el normal funcionamiento de los ordenadores, sin el permiso o el conocimiento del usuario; habitualmente reemplazan archivos ejecutables por otros infectados.
4 ames, Adams: La próxima guerra mundial, pp.15-16, editorial Granica, Buenos Aires (Argentina), 1996.

Los nuevos conflictos de esta era han dado lugar a la denominada guerra de la información, donde se ataca al sistema (Comando, Control, Comunicaciones etc.) desarticulando así sus capacidades, generando así cambios radicales en la naturaleza de los sistemas militares.

Los modernos sistemas de comunicaciones digitales que pueden extenderse a todo el mundo y retransmitir información de ancho de banda amplio en tiempo casi real están cambiando la naturaleza misma del comando y el control (C2).

Estas tecnologías brindan a un comandante dentro de un Teatro de Operaciones, herramientas de avanzada que facilitan su trabajo, permiten tener una visión general de lo que ocurre, contar con un alto grado de certidumbre de lo que va a ocurrir y así poder tomar las decisiones correctas que le permitirán cumplir con su misión.

Si bien estos medios son una de las principales formas para que un comandante reciba información, esta irá evolucionando en forma constante ya que frente a él se encuentra otro ser pensante con las misma necesidades pero con intereses opuestos que tratará por todo los medios impedir que cumpla sus objetivos y, por tal motivo, intentará transferir la incertidumbre y negar el conocimiento a su oponente. Cuanto más rápido nosotros podamos procesar esa información más rápido podremos decidir cómo y cuándo actuar en el combate.

En definitiva, el objetivo es darle al comandante una visión real del desarrollo de las operaciones, lo que permitirá a este tomar decisiones con un mínimo riesgo para sus fuerzas, permitiendo con esta nueva forma de llevar a cabo una guerra, influenciar en forma directa en las decisiones del adversario antes que se lancen las operaciones armadas.

Desarrollo

Influencia de las Nuevas Tecnologías en el C3I2

Las tecnologías de la información actuales y en desarrollo proporcionan una capacidad de comando y control ampliamente mejorada, la cual, por supuesto, tiene tanto ventajas como desventajas. Una ventaja clave es la capacidad de los líderes políticos y militares de más alto rango para seguir el desarrollo de una operación y evaluar el impacto y la eficacia de las operaciones en un tiempo real.

Esto permitirá adoptar decisiones basadas en información actual y precisa y difundir esas decisiones a todos los niveles de comando necesarios en forma rápida y segura. Una de las desventajas más notorias es que la guerra de información involucrará una creciente cantidad de actores, esto podrá dilatar o afectar el proceso para la toma de decisiones.

Para ello los elementos y órganos de comando, operativos, logísticos y servicios

de apoyo, necesarios para cumplir cualquier misión militar que forman un conjunto variado y complejo, 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, requerimientos o información a los otros elementos.

Las actuales tecnologías utilizadas en los sistemas de comando y control, proporcionan al comandante de un teatro la información convenientemente procesada, una imagen actualizada de la situación y con el panorama completo de la zona de operaciones con todos los elementos desplegados. Esto le permite ordenar los esfuerzos, emplear los efectivos disponibles y aplicar los medios adecuados, con precisión, exactitud y conocimiento real del entorno y de las intenciones del enemigo.

Si le sumamos al comando y control, las comunicaciones, la inteligencia y la informática formamos lo que se conoce como C3I2, en su conjunto, estos sistemas entregan a los comandantes una visión acabada del campo de batalla, incluyendo terreno y clima, dispositivo de las fuerzas propias (tamaño, ubicación, dirección de empleo, estado operacional, logística) y dispositivo del enemigo con idéntico detalle.

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. El artículo "La innovación, clave en los Sistemas de Mando y Control de Defensa" del Director de Desarrollo de Negocio y Relaciones Institucionales, Homeland security and Defense José Prieto, hace referencia a como el campo de combate moderno a impuesto mayor rapidez en las operaciones, eficiencia y capacidad de respuesta ante situaciones críticas. Establece que la forma más adecuada para hacer frente a estas exigencias es con nuevas tecnologías.

Este ámbito no consiste solamente en un comandante y su infraestructura para comunicar órdenes, sino abarca todas las capacidades, los procesos de pensamiento y acciones que permitan al mismo observar correctamente la evolución de las operaciones, para realizar evaluaciones y determinar modificaciones oportunas y eficaces, comunicando estas decisiones a los comandos subordinados con el fin de controlar el curso de una operación.

Estos cambios, a su vez, deben ser observados, evaluados por los receptores y actuar en consecuencia generando así un proceso continuo, este proceso puede ser pensado como un "ciclo de decisión" en el cual las operaciones sobre el Comando y Control del enemigo tendrán como finalidad anular, influenciar, perturbar o retrasar este ciclo, pudiendo invalidar de esta manera el desarrollo de las operaciones. De aquí entonces la importancia vital de proteger el sistema de cualquier agresión o interferencia que podría cancelar el empleo de las FFAA con

la anulación o interferencia del propio C3I2.

En relación con estas tecnologías, en EE.UU diseñaron la estructura C4ISR (Comando, Control, Comunicaciones, Computación, Inteligencia, Seguridad y Reconocimiento) en su Visión Conjunta 2010, que provee ventajas de procesamiento de información y comunicación a través de una red de sensores que permite un conocimiento del campo de batalla en tiempo real hasta un espacio de 300 km.[5]

Aquí es donde el concepto C4ISR 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.

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 Fuerzas Armadas (tierra, aire, mar), incluso de nacionalidades diferentes, optimizando el uso de recursos militares. Su objetivo es obtener 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" [6].

Llegados a este punto debe advertirse que el valor de la información no se genera hasta el final de la última milla, y es aquí donde los sistemas C4ISR adquieren toda su razón de ser.

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.

A 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 recur-

5 http://www.afcea.org.ar/publicaciones/conciencia.htm

6 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.

sos que ofrecen hoy las tecnologías de la información, con un control eficiente de los costos.

No obstante, en los últimos años, y reproduciendo la evolución 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 Servicio (SOA en inglés), esta arquitectura permite crear sistemas altamente escalables, que pueden ayudar a las organizaciones a impulsar el rendimiento y, al mismo tiempo, reducir costos y mejorar la flexibilidad en los procesos del negocio. De este modo, conectando adecuadamente los diferentes sistemas, 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 capacidad disponible en red (NEC en inglés).

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.[7]

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

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.

No obstante, existen además, otros requisitos que deben tenerse en cuenta durante la fase de diseño de los sistemas, como es el de la seguridad. En una época en que la ciberseguridad es un asunto de especial preocupación, los elementos de interoperabilidad pueden causar en determinadas ocasiones consecuencias perjudiciales

7 IBIDEM

para la seguridad general de las TIC del sistema y, por tanto, habrán de valorarse adecuadamente.

Actualmente, existen empresas en el mercado que han realizado una labor muy importante de innovación, 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 batalla. Estos sistemas proporcionan al mando una mejor conciencia situacional y mayores herramientas de ayuda para la toma de decisiones.[8]

Estos son algunos de los diferentes sistemas que actualmente podemos encontrar en el mercado:

- TALOS es un sistema completo para el control unificado de los apoyos de fuego de Artillería, Morteros y Naval, diseñado para satisfacer los requisitos NEC de las fuerzas terrestres. TALOS puede personalizarse para diferentes niveles (Compañía, Batallón, Brigada, etc.) y proporciona la automatización de todas las operaciones en el campo de batalla.

- DSC2S es un sistema C4ISR para el soldado a pie (que actúe por sí solo o

8 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 un escuadrón 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. DSC2S permite al soldado operar en el campo de batalla digital no solo como plataforma de armas, sino también como célula sensor de inteligencia y de adquisición de objetivos.

- 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. El LCC2S proporciona capacidades de control en tiempo real y asegura la adecuada gestión de todo el flujo de información necesario para las unidades implicadas. Durante la planificación, 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 síntesis, "la innovación es un factor fundamental, ya que sin ella no obtendríamos la transformación tecnológica actual, que ha experimentado el campo de batalla." [9]

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 vital para lograr el dominio de la situación, de aquí la aplicación masiva de los avances tecnológicos, no sólo procedentes de la investigación y desarrollo militar, sino también como se ha expresado, 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 C3I2 consigue integrar puestos de comando, terminales de información y sensores en localidades remotas, con rapidez y facilidad, con tal de disponer en esos puntos de un enlace por cualquier medio de comunicación.

Las fuerzas que utilicen las posibilidades de este «sistema de sistemas» (acción conjunta de todos los equipos) podrán lograr el dominio de la información, lo cual les permitirá evaluar con precisión las operaciones de las fuerzas propias y enemigas dentro de la zona de operaciones. Aunque esto no elimine la «niebla» de la lucha (sinónimo de incertidumbre), el dominio de la información mejorará el conocimiento de la situación, reducirá el tiempo de repuesta y hará que el escenario del combate sea considerablemente más transparente para quienes posean aquel dominio.

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,

9 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.

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 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 C3I2. 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.

La guerra de información ofensiva reduce, elimina o distorsiona los datos del adversario. Incluye métodos, tanto tradicionales (ataques de precisión para destruir la capacidad de comando y control del adversario) como no tradicionales (intrusión electrónica en sus redes de información y control) para confundir o engañar a los enemigos responsables de las decisiones.

El esfuerzo para lograr y mantener la superioridad de la información lleva consigo también el poder superar con éxito los ataques enemigos a nuestro sistema de información. Como consecuencia, la guerra defensiva para proteger nuestra capacidad de conducir las operaciones de información será uno de los mayores retos para el futuro.

Aquí habrá que incluir a la 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. Ello impone la necesidad de elaborar programas de nivel estratégico que tengan por finalidad proteger esta función crítica en las operaciones. [10]

Los sistemas de comando deben mantener su capacidad operativa en todo momento, incluso a pesar de los ataques enemigos. Para ello es esencial la creación en el personal de una cultura de la seguridad de la información a lo largo y a lo ancho de toda la estructura orgánica. Conviene saber que el ataque informático es más fácil que la defensa y que los agresores cibernéticos atacan los puntos más débiles de la defensa del adversario.

Un sistema de comando debe ser capaz de integrar con rapidez y facilidad tantos puestos de comando, terminales de información y sensores como sean necesarios para el desarrollo de las operaciones previstas en los planeamientos conjuntos y combinados, en localidades remotas y condiciones precarias muchas de las veces.

10 IBIDEM

Para ello deben tener una arquitectura adecuada, capacidad suficiente y facilidad para la integración en el sistema con tal de disponer de un enlace por cualquier medio de comunicación.

Durante la segunda Guerra del Golfo en el 2003, en las doctrinas de empleo de las FFAA estadounidenses en este conflicto, predominó la idea de interferir las comunicaciones y radares iraquíes. Esto facilitó hacerse del control total del espectro electromagnético dejando "ciegos" e incomunicados a los defensores, aislando de esta manera a las tropas desplegadas en el terreno sin poder recibir ningún tipo de orden de sus mandos naturales, generándoles así una incertidumbre total sobre lo que estaba ocurriendo y sobre cómo debían seguir operando.

Conforme a ello podemos decir que esta intervención total en el Comando y Control (C2), llevada a cabo por las fuerzas de EE.UU, ha sido el puntapié inicial para una nueva forma de guerra donde los medios tecnológicos darán, para quien los posea, una gran ventaja en esta nueva tendencia de conflictos que buscan poco daño material, corta duración y un mínimo de bajas humanas.

Conclusiones

La información juega un papel significativo en la Seguridad y la Defensa, que será cada vez mayor por su importancia en un entorno estratégico y táctico dinámico y en continua evolución y que irá presentando nuevos desafíos.

Desde la guerra de Vietnam hasta la última operación del Golfo Pérsico la influencia de la información durante una contienda ha ido ganando mayor preponderancia ayudando en victorias y favoreciendo derrotas en su evolución.

En la actualidad las Tecnologías de la Información y de las Comunicaciones, son imprescindibles para la actuación de las Fuerzas Armadas, tanto en los escenarios tácticos como en los estratégicos, determinando en muchos casos la viabilidad de las operaciones y la superioridad militar.

Por lo tanto dotar a los Ejércitos con sistemas de comando apropiados, además de prepararlos con personal cualificado, 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 sistemas de comando deben poder integrarse de modo que produzcan el intercambio de información conveniente, funcionar con garantía de seguridad y permitir el establecimiento de cuantos puestos sean necesarios en los órganos y unidades de las Fuerzas Armadas, para que, operando con rapidez, coherencia y de forma coordinada, puedan estar siempre en ventaja sobre sus adversarios.

En consecuencia si bien existen diversas formas de definir a la Guerra de la Información, todas coinciden en la influencia en que esta nueva forma de combate

permite a un comandante la posibilidad de observar dentro de un Teatro de Operaciones en forma inmediata, el terreno, clima, dispositivo de las fuerzas propias (tamaño, ubicación, dirección de empleo, estado operacional, logística) y del dispositivo del enemigo con idéntico detalle.

Las NEC por ende permitirán compartir información en red para su empleo en operaciones y así obtener una supremacía en el combate, mediante el predominio en la información, en el conocimiento y en la decisión, lo que ha originado un nuevo modelo de mando y control caracterizado por su descentralización. Este nuevo tipo de mando y control permite una mejor comprensión de la situación y por lo tanto logra mayor eficacia en el cumplimiento de la misión, al acortar el tiempo necesario para la toma de decisiones y la sincronización de las acciones.

El Coronel Robert Ballew, Jefe del Tercer Batallón de AH-64, perteneciente al 229 Regimiento de Helicópteros de Ataque con base en Fort Bragg, en su ponencia en el Seminario NEC, organizado por el Centro de Excelencia de Mando y Control de la OTAN en 2007, expuso que durante la operación Libertad Duradera en Afganistán el sistema de información (*blue force tracke*r) aceleró la toma de decisiones al proporcionar una visión compartida de la situación de las unidades propias; además, el uso intensivo del *chat* entre unidades colaterales por parte de los oficiales y suboficiales de menor graduación permitió aumentar el apoyo recíproco de una forma casi instantánea acelerando el proceso de sincronización de las operaciones.

Para lograr la compatibilidad de un moderno sistema C3I2, y la necesidad de comunicación a través de las distintas redes desplegadas, es necesario lograr crear conciencia de las medidas de contra inteligencia en nuestro personal, debido a que no podemos afirmar que por más altamente desarrollados estén los sistemas de vigilancia y control de nuestras comunicaciones, el hombre termina siendo habitualmente el eslabón más débil de la cadena. Asimismo, este sistema representa un paso más en la relación entre el hombre y la tecnología, fomentando la colaboración a distancia fuera del ámbito estrictamente profesional, en este caso el cultural, mediante herramientas de avanzada tecnología.

Los avanzados sistemas de C4ISR de las potencias mundiales, acompañados de sus modernas tecnologías ofrecen el potencial que permiten empeñar las fuerzas militares con mayor eficacia. No obstante, se debe tener claro que no se está frente de una renovación de material que se usa para hacer la guerra, sino que se está frente a una genuina revolución cultural, que implica, la forma en que se hace la guerra.

La tendencia de llevar adelante guerras de corta duración y con un mínimo de bajas humanas, dan un marco ideal para este tipo de conflictos donde operando a través de los ámbitos de Comando y Control, Acción Psicológica, Inteligencia, Guerra Electrónica, Ciberguerra y el engaño militar podemos alcanzar objetivos militares sin el despliegue de fuerzas militares y a un costo mínimo pudiendo

ocasionar los mismos efectos que una tropa convencional.

Estas nuevas tendencias que hoy parecen sorprendentes seguramente son el preludio de lo que vendrá en los próximos años, al ritmo que evoluciona la tecnología no podemos prever cuales y como serán los nuevos desarrollos y los modos de aplicaciones, lo que si podemos estar seguros que hasta ahora solo vimos la punta del iceberg de la Guerra de la Información.

Bibliografía

- Adams, James: La próxima guerra mundial, pp.15-16, editorial Granica, Buenos Aires (ARGENTINA), 1996.
- Los ámbitos no terrestres en la guerra futura: ciberespacio - centro superior de estudios de la defensa nacional – Editado por el Ministerio de Defensa Español –. REINO DE ESPAÑA, Mayo 2012.
- Mayor Elizabeth L Robbins. Revista Ejército de EEUU. Las operaciones de Información con botas en el terreno: El auge del blog militar. Manual de Informaciones ESTADOS UNIDOS DE AMERICA, Octubre-Diciembre 2008.
- Pedro Sánchez Herráez Comandante Infantería DEM. Guerra de cuarta generación y las redes. Revista Ejército de tierra español. REINO DE ESPAÑA, Noviembre 2008.
- 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. REINO DE ESPAÑA, Enero 2012.
- La función de Mando y Control en la Guerra de Maniobra. Rubén SEGURA FLORES Teniente Coronel Ejército de Chile - Profesor del Departamento de Estudios Estratégicos de la Academia de Guerra del Ejército. Revista Memorial ECH Setiembre 2011.
- Nuevas Tecnologías en Mando y Control. Francisco José Oliva Bermejo. Comandante de Transmisiones. DEM. Revista Ejército N. 836. REINO DE ESPAÑA, Diciembre 2010.
- Minoletti Olivares, Jorge Guerra de la Información Disponible en: http://www.afcea.org.ar/publicaciones/infoguerra2.htm

Currículum Vitae del TCnl Roberto Claudio Galizia

Es Oficial de Estado Mayor del Ejército Argentino y Diplomado en Altos Estudios Nacionales del Estado Plurinacional de Bolivia. Es Licenciado en Estrategia y Organización, Magister en Defensa, Desarrollo y Seguridad y Magister en Educación Superior. Se desempeñó como profesor en el Colegio Militar del Ejército "Cnl. Gualberto Villarroel" y en la Escuela Militar de Inteligencia "Gral. Ejto. Joaquín Zenteno Anaya" de Bolivia. Fue 2do Jefe de la Base Antártica Esperanza, Jefe de la Compañía de Comunicaciones Paracaidista 4 y Jefe del Batallón de Comunicaciones 141. Actualmente se desempeña como profesor en la Escuela Superior de Guerra.

Este artículo trata sobre el tratamiento de la Ciberdefensa desde el Derecho Internacional Público por parte de la OTAN a partir de la publicación en 2013 del "Tallin Manual on the International Law Applicable to Cyber Warfare", constituyéndose en la primera definición en materia de Derecho de los Conflictos Armados y por ende con incidencia en la Seguridad Internacional.

El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra

Autores: Dra. Claudia Elizabeth Fonseca, My (Aud.) Ivonne Luz Perdomo,

Lic. Miguel Arozarena Gratacos y Dr. Javier Ulises Ortiz

Proyecto de Investigación "Ciberdefensa" de la ESG

Propósito

Una apreciación del Manual de Tallin de la OTAN tanto estratégica como jurídica resulta necesaria para encuadrar las acciones ofensivas y defensivas de actores en el ciberespacio, lo que requiere un encuadramiento normativo de la dinámica de los conflictos en ese nuevo ambiente operacional signado por lo tecnológico, siendo esta la primera en su tipo.

Introducción

En un mundo cada vez más interrelacionado por el denominado proceso de globalización e incrementado por el "cuatro espacio" o el ciberespacio, las Políticas de Defensa de los Estados constituyen un factor preponderante para la materialización de alianzas y proyectos en conjunto que aseguren el desarrollo de las mismas acordes al nuevo escenario mundial. Así, las Políticas de Defensa comienzan a atender cada vez más al concepto de "fronteras virtuales" como una expresión normal para la interacción que se produce en el sistema internacional. La función de la Defensa es similar para las distintas naciones, tendiendo como objetivo prioritario mantener la Soberanía y la integridad territorial.