Desarrollo aplicación y dominio de tecnologías de comunicación en operaciones militares de alto riesgo

Michel Alexander Carreño Vargas
Edison Alexander Torres Leiva
William Gilberto Guevara Guevara
Nestor Andrian Guarnizo Rojas

Trabajo de grado para optar al título profesional:
Curso de Estado Mayor (CEM)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2011

355.4005
D371

FUERZAS MILITARES DE COLOMBIA

ESCUELA SUPERIOR DE GUERRA

DESARROLLO APLICACIÓN Y DOMINIO DE TECNOLOGÍAS DE COMUNICACIÓN EN OPERACIONES MILITARES DE ALTO RIESGO

MY. MICHEL ALEXANDER CARREÑO VARGAS 79´601.997
MY TORRES LEIVA EDISON ALEXANDER 79´625.755
MY. GUEVARA GUEVARA WILLIAM GILBERTO 80´439´618
MY. GUARNIZO ROJAS NESTOR ANDRIAN 18´183.913

AULA "F" CEM 2011

ASESOR:

DR. ANDRES GAITAN

Bogotá D.C.

09 de agosto de 2011

TABLA DE CONTENIDO

DESARROLLO APLICACIÓN Y DOMINIO DE TECNOLOGÍAS DE COMUNICACIÓN EN OPERACIONES MILITARES DE ALTO RIESGO

INTRODUCCION

El propósito de esta investigación es dar a conocer las diferentes maneras en que se desarrollan acciones dentro de la guerra de información, donde encontramos conceptos como ciberterrorismo, ciberguerra y ciberdefensa entre otros, y, que a través de los años y el transcurrir del tiempo se manejan en formas diferentes pero con un mismo objetivo e ideal: garantizar el privilegio de manejar la información de manera veraz y oportuna brindando ventajas de tiempo para la toma de decisiones lo cual la convierte en un recurso estratégico de vital importancia en los conflictos cuya base son los desarrollos tecnológicos de alta precisión.

En las guerras de información encontramos un desarrollo vertiginoso, que está afectando a todos los campos de nuestra sociedad, las tecnologías cada vez más se presentan como una necesidad en el contexto de sociedad donde los cambios, el aumento de los conocimientos y las demandas de una educación de alto nivel constantemente actualizada se convierten en una exigencia permanente que garantiza, el privilegio de manejar la información de manera veraz y oportuna brindando ventajas de tiempo para la toma de decisiones lo cual la convierte en un recurso estratégico de vital importancia en los conflictos cuya base son los desarrollos tecnológicos de alta precisión.

Estos hechos a lo largo de la historia y análisis de determinados conflictos de orden mundial han atraído la atención de la opinión pública en general por la manera en que evolucionaron y los resultados que se obtuvieron con implementaciones de nuevas formas de hacer guerras mediante el empleo de nuevas y variadas herramientas que generan resultados y efectos

diferentes según el contexto en que se desarrollen. Si se revisa los conflictos bélicos del siglo XX y los vividos en esta primera década del siglo XXI, vemos que el concepto de "guerra" ha cambiado drásticamente en estos cien años. Lo único que se sigue manteniendo igual es que la población civil es la que se lleva la peor parte[1].

El hombre siempre ha tenido una habilidad muy especial para hacer la guerra. Desde la época de las cavernas, nuestros antepasados se las ingeniaron para convertir un pesado hueso o piedra en un arma para cazar animales o congéneres. A medida que la civilización fue conquistando nuevas áreas de conocimiento, invariablemente fueron puestas al servicio de la guerra: desde el fuego y la rueda hasta la pólvora y el telescopio, desde el motor a vapor hasta el ordenador, todos, sin excepción, se utilizaron para obtener una ventaja en el campo de batalla.

El amplio espectro de cambios producidos en las formas de conducción de los conflictos armados, comprende estrategias, no tradicionales e inquietantes desde el punto de vista de la política y de la conducción de la seguridad del estado, como una situación de garantía y tranquilidad propiciada por el poder nacional, de ahí se facilitan las técnicas y metodologías comprendidas en la aplicación, adquiriendo conocimientos sobre componentes, fundamentos organizacionales y técnicos de los sistemas de información, así como los ciclos de vida y metodologías del desarrollo adecuado combinando una serie de modelos, métodos, técnicas, metodologías y herramientas para el análisis y el diseño de sistemas de información.

[1] Neoteo. Ciberguerra. (en línea) Disponible en http://www.neoteo.com/ciberguerra-la-guerra-que-viene. Consultado el 10 de junio de 2011.

Hay que distinguir, por una parte, los medios como instituciones sociopolíticas, y por otra, los contenidos como material simbólico formado por diferentes tipos de mensajes, distinguiendo dentro de éstos entre información y opinión pública, entretenimiento y ficción, y publicidad y propaganda. Dentro de estos contenidos se ve reflejado el grado de influencia, término que debe entenderse desde una situación social de la vida colectiva donde los sujetos de cualquier grupo están obligados a relacionarse para cooperar, de modo que es imprescindible que exista influencia de unos sobre otros al tener que adaptarse entre sí.

Por la gran influencia en la opinión y los hábitos de la gente, son el objetivo de gobiernos y empresas, los que de una u otra manera han ayudado de manera decisiva al proceso de globalización, puesto que permiten que cualquier persona pueda acceder a la información de cualquier lugar en cualquier momento, y cada vez con mayor rapidez, por lo que han colaborado en la expansión y estandarización de los gustos culturales de la población mundial. Siendo objeto de disciplinas muy diversas, desde la sociología hasta la economía, pasando por el arte y la filosofía[2].

El avance tecnológico de la época en que se vive, la capacidad de los militares en las operaciones de información incluyen la guerra en técnicas de información y comunicación en las operaciones militares, la desinformación militar y la seguridad de operaciones; son coordinadas y estrechamente concentradas ya que estas capacidades pueden disuadir el conflicto. Se sabe que los Ejércitos de todo el orbe usan elementos sofisticados de empleo para la conducción estratégica y táctica para la administración de personal y medios frente a los Estados modernos, con organizaciones muy complejas, en donde la comunicación instantánea en todo el mundo entre las

[2] García Fajardo, J.C. (1992-05-26): Comunicación de masas y pensamiento político http://www.educacionplasticavisual.es/?cat=5 Consultado el 25 de julio de 2011.

fuerzas aéreas, marítimas y terrestres es fundamental para las operaciones militares[3].

Al hablar de seguridad y defensa nacional, encontramos un factor que trasciende las fronteras y es la base legal que garantiza que los estados, tengan las herramientas necesarias para poder emplear a las instituciones armadas y a los organismos de seguridad pública y los organismos de inteligencia, donde se permita jugar un papel importante en el manejo de la información de las amenazas crecientes.

De esta forma, las operaciones militares (...), cuentan rápidamente con ganar cualquier enfrentamiento cinético, desde el comienzo, para llevar a cabo las operaciones de información con la misma capacidad y un desarrollo constante que si bien, está favoreciendo a las sociedades de nuestro hemisferio, también se convierten en una amenaza. La tecnología juega un papel importante, no es por sí sola, de utilidad sino tiene que ir ligada a los medios tecnológicos utilizados por una nación, de un conglomerado para que pueda garantizar su progreso, de prosperidad, seguridad y bienestar, pueden ser utilizados para bien de la nación[4].

En este orden de ideas, las redes informáticas contra una red de comunicaciones del Estado, puede impedir, deteriorar o interrumpir su uso para fines de mando y control de las Fuerzas Militares, o su uso por parte de los líderes claves a fin de coordinar una respuesta nacional. Las operaciones de apoyo en la información militar son eficazmente empleadas, como una capacidad integrada que puede disuadir el conflicto armado tanto con

---

[3] Reig, Ramón (1995): El control de los medios de comunicación de masas: bases estructurales y psicosociales http://www.laislalibros.com/libros/control-de-la-comunicacion-de-masas

[4] APPLEGALE MELISA, Informe publicado sobre Ciencia y Tecnología publicado por El Stralegre Studies Institute, septiembre de 2001.

posibles adversarios estatales como los no estatales, teniendo en cuenta que la habilidad de justificar el uso de las operaciones de información no constituye el uso de la fuerza en el sentido tradicional.

Las capacidades militares básicas de las operaciones de información incluyen la guerra electrónica, las operaciones de redes informáticas, de apoyo de información militar, des-información militar y la seguridad de operaciones, las cuales son debidamente coordinadas y estrechamente concentradas, porque pueden disuadir el conflicto armado. Los medios tecnológicos y la gestión de información generan un nuevo conocimiento jugando un papel prioritario en el éxito o el fracaso de las actuaciones de las fuerzas y cuerpos de seguridad del Estado, en el ámbito de la prevención por medio de la información.

La "(...) evolución tecnológica, especialmente en los últimos quince años, ha provocado en el ámbito militar una verdadera Revolución de los Asuntos Militares (RMA), al aplicarse dichos desarrollos, no sólo al perfeccionamiento de los sistemas de armas tradicionales sino a nuevas formas de empleo del poder militar. La incorporación de innovaciones tecnológicas y el uso inteligente de las mismas, reforzadas con cambios orgánicos y doctrinales, permitió aumentar la capacidad de combate contra adversarios estructurados y renuentes a los cambios"[5]. Sin lugar a dudas, el avance tecnológico se ha presentado en forma significativa, y sobre todo en el campo de batalla moderno, el cual se ha visto influenciado por el acelerado ritmo de las operaciones, en que la función de Inteligencia tiene que interactuar con modernas tecnologías para cumplir su misión[6].

---

[5]Asociación Internacional de Comunicaciones y Electrónica de las Fuerzas Armadas (AFCEA Internacional). AFCEA Argentina (En línea) http://www.afcea.org.ar/cursos/OpInfo.htm. Consultado el día 24 de abril de 2011.

[6] MATAMALA APARICIO Salvador, Guerra de la Informática, monografías Chile 13 de enero de 2009. http://www.ufro.cl/corporativa/docs/Memoria%20Institucional, 20 UFRO/202/06.

Esta obtención de información, al procesarla, ha colocado una gran división entre el discurso de la comunicación y los medios masivos, se vuelve complicado para un número de pequeñas sub-áreas de los estudios en comunicación, lo que incluye la comunicación intercultural e internacional, los pequeños grupos de comunicación, las tecnologías de la información y la comunicación, son cobijadas por las políticas, marcos legales de la comunicación, las telecomunicaciones y el trabajo en otros niveles variados han logrando la interpretación y el procesamiento de datos, a reducir la incertidumbre acerca de los sucesos sobre la información[7].

El desarrollo de las redes informáticas ha posibilitado su conexión mutua y, finalmente, la existencia de Internet, una red de redes, permitiendo a una computadora intercambiar fácilmente información con otras situadas en regiones lejanas del planeta.

La superioridad en el manejo de la información permite dar aplicabilidad a un nuevo concepto en los principios de la guerra como lo es la opinión pública, que manejada hábilmente puede generar reveses en los objetivos políticos y militares del adversario, casos como la administración de los medios de comunicación pueden generar en la población presión para obligar la toma de decisiones que favorezcan a una parte o la otra según sean los intereses que se manejen. De igual forma con un dirección adecuada se puede revertir el pensamiento de una comunidad y que sea ella la que públicamente intervenga y evite acciones de mayor intensidad al verse vulnerada.

En la globalización informática, no existe una sola fuerza que decida todo, como tampoco es posible apelar al modelo de emisor–receptor de la comunicación. La llamada "sociedad de la información o era de las

---

[7] BARRIOS EDGARDO Martin, Profesor Universitario en Informática aplicada – Facultad de Ingeniería, Universidad Nacional del Chaco – Argentina. www.answers.yahoo.com/question/index

comunicaciones" se refiere al achicamiento del mundo, a la erosión de todo tipo de fronteras y a la reconfiguración de los mecanismos de decisión quiénes emiten los mensajes y los cuales, al igual que otros medios, gobiernos, empresas, capital transnacional, o personas individuales[8].

La cultura cibernética se adapta a esta definición tanto por la cultura en sí como por el medio que la trasmite en un reconocimiento, que se conoce como realidad virtual. En donde se resalta específicamente dónde y cuándo inicio el desarrollo de los procesadores o computadores informáticos, y la Internet[9].

A las redes se les llama el "ciberespacio" y a sus usuarios navegadores, ya que este medio alternativo a creado precisamente eso, un espacio cibernético donde cualquier persona de cualquier parte del mundo puede navegar en él por medio de una computadora y una conexión como la línea telefónica, cable, medio inalámbrico, ha venido a crear nuevas formas de comunicación e intercambio cultural y de ideas sin olvidar por supuesto la forma de realizar compras o hacer negocios[10].

Las amenazas informáticas de un país no solo provienen de otro Estado, pueden estar también conformados por empleados de las mismas instituciones gubernamentales, adolescentes que desean probar su alcance en la red, hackers y organizaciones terroristas, entre otras, que buscan acceder a lugares no autorizados para obtener información o efectuar daños mediante la introducción de virus o programas que pueden ser de espionaje

---

[8] TREJO DELBARNE, Raúl: La nueva alfombra mágica. Usos y mitos de Internet, la red de redes.
http://www.nua.ie/surveys/how_many_online/index.html

[9] Publicaciones de la RED en.medi@:en.re.dando: http://www.enredando.com

[10] Francia. Presseurop.eu. Ciberdefensa Estonia forma un ciber ejército (en línea) http://www.presseurop.eu/es/content/news-brief-cover/462031-estonia-forma-un-ciber-ejercito-modification. Consultado el día 20 de abril de 2011.

para engaño, negación de información o de daño y pérdida total de la misma; perdiendo confidencialidad y credibilidad al interior de las organizaciones involucradas.

El internet, proporciona medios baratos y eficaces, para que el terrorismo, sea una fuente inagotable de documentación de interconexión, los cuales a través de la red los líderes terroristas son capaces de mantener relaciones con los miembros de la organización u otra sin necesidad de tener que reunirse físicamente, tal es así que, los mensajes vía correo electrónico se han convertido en la principal herramienta de comunicación, (...) para financiarse, reclutar nuevos miembros, adiestrar a los integrantes de las distintas células, comunicarse, coordinar, ejecutar acciones, encontrar información adoctrinar ideológicamente, promocionar sus organizaciones y desarrollar una guerra psicológica contra el enemigo es decir, como un medio para recaudar fondos para la causa[11].

El problema que se plantea es que el internet carece de fronteras es el intercontenido ilícito que circula de un país a otro en milésimas de segundos; además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a internet y otras donde de forma anónima las personas pueden conectarse y realizar actividades lícitas e ilícitas.

EL USO DEL INTERNET Y LA INFLUENCIA EN LAS TECNICAS INFORMATICAS Y DE COMUNICACIÓN EN LAS OPERACIONES MILITARES

---

[11] Ibíd.

El Internet, nacido como espacio de intercambio de información entre científicos europeos, ha adquirido un auge estratosférico en los últimos años pasando del comercio electrónico (e-commerce) de IBM a los negocios electrónicos utilizados inicialmente por empresas de Estados Unidos de Norte América como Dell, Yahoo y Ebay, así como a espacio de comunión entre miles de personas alrededor del mundo. Internet ha venido a crear nuevas formas de comunicación e intercambio cultural y de ideas sin olvidar por supuesto la forma de realizar compras o hacer negocios[12].

Operaciones miliatres es un concepto, y no debe confundirse con las operaciones militares como sucesos, engloba la planificación y movilización de las fuerzas militares, del proceso de recogida de Inteligencia, del análisis y extensión de la Información, asignando recursos y determinando los requerimientos temporales. Una operación militar puede implicar el desarrollo de una estrategia militar o de una maniobra operacional a través del uso del movimiento logístico de fuerzas. En general, el término en tácticas militares se usa al referirse a operaciones de combate militares en misiones militares, que son un subconjunto de las operaciones militares.

En el proceso de desarrollo de la operación las fuerzas pueden requerir la provisión de servicios, entrenamiento, o funciones administrativas para permitirles comenzar, continuar y terminar el combate, incluyendo la dirección del movimiento, suministros, ataque, defensa y maniobras necesarios para conseguir los objetivos de la operación en una batalla o campaña[13].

---

[12] Del El Diario Digital: Edición Cd. Juárez. Toman Adicción por Web. 18 de Noviembre 2005.
[13] ARMSTRONG, Richard N. Red Army Tank Commanders: The Armored Guards. Atglen, Penn.: Schiffer Military History, 1994.

La instrucción militar busca formar a los ciudadanos para Asegurar la Defensa Terrestre, contribuir con la estabilidad de las Instituciones Democráticas y el respeto a las Leyes de la República, apoyar la Integración y el Desarrollo Nacional y estar preparados para participar en programas de cooperación y mantenimiento de la Paz Internacional.

En lo que se refiere a la producción de la información en tiempos de guerra las estrategias y las tácticas de la comunicación Militar, interfieren simultáneamente y se hacen participes de las formas de operación mediática de las sociedades democráticas en las que los medios funcionan como empresas.

Si se aplica esta distinción al caso de una confrontación armada quiere decir que los ejércitos comunican, mas no informan, su meta, en las relaciones que establecen con los medios de comunicación; no es buscar la "verdad" de los hechos, ni describir la "realidad" para la población, sino que se trata de ganar una guerra al menor costo posible. Mientras que el trabajo de los medios consiste en informar y ganar ventaja comercial a los otros medios, el trabajo de los ejércitos es ganar la guerra política[14].

Uno de los logros más importantes y claros dentro la ejecución de las operaciones militares y civiles, son las que pueden clasificarse mediante la escala y el alcance de la fuerza empleada, y por su impacto en un conflicto más amplio.

ALCANCE DE LAS OPERACIONES MILITARES

[14]G charon, J-M., Mercier, a. (coord.). (2004). Armes de communication massive. Information's de guerre en Irak: 1991-2003. Paris: cnrs Editions.

Teatro: esto describe a una operación en un área de operación más grande, a menudo a nivel continental, y representa un esfuerzo estratégico nacional en el conflicto, tal como fue la Operación Barbarroja, con objetivos generales que engloban áreas de consideración más allá de lo militar, como son objetivos de impacto económico y político[15].

Campaña: esto describe una de dos, o a una parte del teatro de operaciones, o un esfuerzo estratégico operacional más limitado a nivel geográfico, tal como fue la Batalla de Inglaterra, y no necesita representar un esfuerzo nacional total a un conflicto, o tener objetivos más allá de los que son puramente militares.

Operación: esto describe a una parte de una campaña que tendrá objetivos militares específicos y objetivos geográficos, así como un uso definido y claro de las fuerzas a emplear, tal como fue la Batalla de Galípoli, que operacionalmente fue una operación de armas combinadas originalmente conocida como "Desembarcos de los Dardanelos", y que fue parte de la Campaña de los Dardanelos, en la que tomaron parte unos 480.000 soldados aliados[16].

Batalla: esto describe a un suceso de combate táctico en el que se combate por un área u objetivo específico mediante acciones que realizan las diferentes unidades. Por ejemplo la Batalla de Kursk también conocida por su denominación alemana, como "Operación Ciudadela", en la que hubo muchas batallas separadas, una de las cuales fue la Batalla de Prokhorovka. La "Batalla de Kursk", además de describir la operación ofensiva alemana

---

[15]GLANTZ, David M. Soviet Military Operational Art: In Pursuit of Deep Battle. London; Portland, Or.: Frank Cass

[16]Ejército de Chile, artículo "la logística y la Guerra del golfo Pérsico y la Guerra en Irak (2003), año 2006.

inicial (o simplemente una ofensiva) también incluyó dos operaciones contraofensivas[17].

El planeamiento previo: Cualquier operación militar se inicia mucho antes del despliegue. Antes incluso de que se confirme si habrá una operación militar. Ante los primeros indicios de una posible actuación: estudios de viabilidad de una operación, seguimiento de zonas "calientes" o despliegue de equipos de reconocimiento, el personal militar debe iniciar el seguimiento de las noticias relacionadas con el asunto de forma que una vez que se empieza el planeamiento de la operación se disponga de información suficiente que permita predecir los temas sobre los que la prensa incidirá una vez que se haga público, orientando el plan de comunicación[18].

En el planeamiento general previo de la operación se tiene en cuenta el factor comunicación y personal militar especialista que debe estar integrado en los equipos de planeamiento para confeccionar los apartados relativos a la comunicación, es decir: trato con la prensa, mensajes a transmitir por parte de las fuerzas, momentos de mayor interés mediático, temas previsibles, preparación del personal así como recopilación de datos que solicitará la prensa tales como fechas, personal implicado, equipo, área de despliegue, etc.

Los militares sacan provecho de su rol de fuentes informativas y se preocupan por mantener y reforzar las relaciones personales que cada uno pueda establecer con los periodistas. Todo periodista debe gran parte de su trabajo a sus fuentes informativas, por lo tanto, cuando acude a ellas debe

---

[17]ARMSTRONG, Richard N. Red Army Tank Commanders: The Armored Guards. Atglen, Penn Schiffer Milit .History.

[18]Página web del Ejército de Chile, www.ejercito.cl, comunicados de prensa por ayudas a la población.

velar, a su vez, por mantener una buena relación para en un futuro poder solicitarla.

LAS OPERACIONES MILITARES CON LOS MEDIOS DE COMUNICACION

Las operaciones militares tienen "picos" informativos, en el inicio de la operación suele ser el momento de mayor intensidad y como decía antes debe estar preparado y planeado. Sin embargo, una vez iniciada hay que continuarla proporcionado información de los hechos, las actuaciones destacadas o errores significativos, su relevancia debe ser difundida rápidamente antes de que otras vías que no dispongan del mismo nivel de información puedan "intoxicar" la noticia con repercusiones indeseables.

Para que exista una buena coordinación, el personal de Comunicación tiene que estar permanentemente integrado en los Centros de Operaciones, elemento de los cuarteles generales desde donde se sigue minuto a minuto la operación y a donde llega toda la información. Esta figura resulta fundamental para poder obtener la información de mayor importancia en el momento de producirse.

LOS ENIGMAS DE LA REVOLUCION NAZI EN EL PROCESO INFORMATICO Y LAS COMUNICACIONES EN LAS OPERACIONES MILITARES

El término "Nazi", se deriva de las primeras dos sílabas del nombre oficial del partido: Nationalsozialistische Deutsche Arbeiterpartei o "NSDAP". Los miembros del partido se identificaban a sí mismos generalmente como "Nationalsozialisten" (Nacional socialistas) y solo raramente como "nazis".

El origen y uso de "nazi" es similar al de "Sozi", palabra del lenguaje diario para designar a los miembros del Sozialdemokratische Partei Deutschlands (Partido Socialdemócrata de Alemania). En 1933, cuando Hitler asumió poder en el gobierno alemán, el uso del término disminuyó en Alemania, aunque en Austria sus oponentes lo continuaron usando con una connotación despectiva. A partir de eso, el término ha adquirido una connotación crecientemente peyorativa[19].

La primera guerra mundial marcaría un hito fundamental en la historia de la propaganda ya que a partir de entonces, se convertiría en un proceso organizado y profesionalizado que dejaría significativos aportes en diferentes ámbitos. Es en esta primera guerra cuando aparece el concepto de "Guerra de masas", la guerra, ya no será un acontecimiento que involucraría no sólo a unos cuantos militares sino que afectaría directamente a la población civil.

Alemania es el único país que, una vez involucrado en la primera guerra, utilizó una propaganda de tipo "defensiva" reaccionando a los mensajes difundidos por el enemigo. Esta decisión política sería criticada por Hitler tiempo después. Estos antecedentes hicieron que en el ámbito militar, la propaganda sea entendida como una acción psicológica cuyo objetivo es la "motivación" de los combatientes.[20]

La primera guerra mundial, marcaría un hito fundamental en la historia de la propaganda ya que a partir de entonces, se convertiría en un proceso organizado y profesionalizado que dejaría significativos aportes en diferentes ámbitos. Es en esta primera guerra cuando aparece el concepto de "Guerra

---

[19] Articulo Nazi, en: Friedrich Kluge, Elmar Seebold:Etymologisches Wörterbuch der deutschen Sprache, Walter de Gruyter Auflage, Berlin/New York 2002

[20] CALCAGNO Eduardo, Propaganda, la comunicación política en el siglo XX, Comunicación Gráfica Edición y Diseño, 1992.

de masas", la guerra, ya no será un acontecimiento que involucraría no sólo a unos cuantos militares sino que afectaría directamente a la población civil.

Por primera vez se hablaría de una "Guerra total" ya que, como nunca antes, serían decisivos tanto los recursos humanos como los tecnológicos. Tal es así que, es en esta primera guerra cuando la fabricación de armas bélicas comienza a transformarse en una industria poderosa, la artillería se vuelve sofisticada. Aparecen las ametralladoras y con ellas, la guerra se mecaniza, las trincheras son parte de un nuevo esquema de batalla en el que el enemigo avanza lentamente sobre la debilidad del bando contrario. Hay una enorme cantidad de pérdidas humanas, (...) unas 600,000 personas por cada bando. Ante esta realidad, que pone en evidencia la proximidad de la muerte y jaquea la moral de las tropas, sería la propaganda el recurso que permitiría sostener la motivación de los soldados para la lucha[21].

Como consecuencia del descrédito de la propaganda, cuando en la Segunda Guerra Mundial el gobierno británico intentó sensibilizar a la población sobre la existencia de campos de concentración nazis, esta información no fue tenida en cuenta, porque el público sospechó que era una campaña propagandística más.

Los alemanes, en la Primera Guerra Mundial, fueron derrotados más en el terreno sicológico que propiamente en el campo de batalla. Hitler reconoció la funcionalidad de la propaganda británica, en donde en a partir de 1916 continuó más intensamente, y en el inicio de 1918 se transformó en una nube negra.

---

[21] Kershaw, Ian. (1999) Hitler ISBN 0-393-04671-0 Berlin.

Ahora se puede ver los efectos de la seducción gradual y de ahí que Alemania falló en reconocer la propaganda como un arma de primera utilidad y los ingleses la utilizaron con gran pericia y genial deliberación". Al final, la primera experiencia de los británicos con la propaganda fue entendida como un gran éxito y dio ejemplo para que otros países empezaran a usar las técnicas contemporáneas de comunicación persuasiva.

En la Segunda Guerra Mundial, se asistió a un uso continuado de las comunicaciones, la propaganda como un arma poderosa. Tras el fracaso alemán en entender la propaganda como un aliado esencial, Hitler se preocupó por crear un cargo en su gobierno exclusivamente dedicado a la propaganda. Comparada con los regimen soviéticos y fascista, la propaganda nazi no formaba parte de un todo, sino que era en sí misma el todo, el esquema de proliferación de información falsa en el régimen nazi que pasó a la historia como "la gran mentira".

La propaganda hitleriana y los medios de comunicación difundidos se centraban en un tipo de mensaje emocional que se dirigía, sobre todo, a un público poco educado políticamente, susceptible de interiorizar la emoción y no la racionalidad. A su salida de la cárcel, Hitler aprovechó la prohibición de hablar en público en Alemania para llevar a cabo su primera gran campaña de propaganda, basada en la idea de que entre los 2000.000.000 de habitantes de la Tierra, sólo él no podía hablar en Alemania y sus discursos eran preparados con detalle.

En la actualidad, en un mundo globalizado, la revolución digital proporciona soportes tecnológicos de gran eficacia para la propaganda de guerra. Este factor, unido a la experiencia ganaba desde la Primera Guerra Mundial, potencia para este tipo de comunicación persuasiva, de modo que cabe

preguntarse hasta dónde pueden llegar los peligrosos efectos de la mala aplicación de las técnicas y comunicaciones.

Las distancias geográficas siguen siendo las mismas, la internet, telefonía y la televisión satelital, como las cadenas televisivas mundiales han hecho que la información viaje a velocidades nunca vistas, afectando la toma de decisiones, a la manera de ver el mundo hoy, a la convivencia global y las especialmente relacionadas con las operaciones militares. Estas condiciones llevan a las sociedades a crear un macro centro de intercomunicaciones entre los gobiernos y entidades financieras de los países, crean relaciones mutuas que interconectan rápidamente a las economías mundiales.

Y esto, a su vez genera perspectivas de desarrollo a países que se adaptan rápidamente a nuevas reglas, esta rápida integración de las sociedades hace que se desarrollen áreas especificas en las economías nacionales, como las finanzas, las relaciones comerciales y las comunicaciones, los avances tecnológicos están llegando cada vez más rápido, las cuales ven multiplicadas las posibilidades de sus productos, y con esto se abren nuevos escenarios y descubrimientos de técnicas y tecnologías. "El gran reto de la globalización es que plantea que las sociedades deban adaptarse secuencialmente a las innovaciones a los nuevos escenarios de cambio en las esferas de comunicación y de avances tecnológicos"[22].

La guerra sin duda es un factor que obliga a desarrollar tecnologías que brinden ventajas ante el adversario, ha sido así desde siempre y en la era informática actual no sería esto una excepción. Los escenarios cambian y por supuesto las herramientas para controlar los nuevos contextos deben evolucionar para adaptarse y conseguir el objetivo, la derrota del oponente.

---

[22] MORA PARDO Álvaro, Globalización, Interdependencia compleja y disuasión.

CONCEPTUALIZACIÓN DE LA CIBERGUERRA

Para el tema se encuentra apoyo en el desarrollo de ensayos académicos que soportan el punto de vista fundamentado en argumentos, algunos hechos acaecidos a lo largo de la historia y análisis de determinados conflictos de orden mundial que atrajeron la atención de la opinión pública en general por la manera en que evolucionaron y los resultados que se obtuvieron con implementaciones de nuevas formas de hacer guerras mediante el empleo de nuevas y variadas herramientas que generan resultados y efectos diferentes según el contexto en que se desarrollen.

Las implementaciones de la electrónica y la informática ofrecen avances tecnológicos que cambian a pasos agigantados especialmente en países desarrollados y con suficiente capital para apoyar la investigación. En el primer caso les han permitido llegar a la elaboración y materialización de diseños altamente sofisticados y de tamaños sorprendentes permitiendo con ello fabricar nanotecnologías que cada vez son más imperceptibles por sus diminutos tamaños, fácil camuflaje y gran variedad de aplicaciones; en el segundo caso se encuentra el desarrollo de software avanzados que permiten la filtración y penetración de programas que en muchos casos no son perceptibles por quienes resultan afectados.

Existe además diversidad de interpretaciones respecto a definiciones de ciberguerra, es un término que se encuentra con amplia divulgación en el léxico que se emplea diariamente. A pesar de no tener un componente netamente militar, es un área de aplicación que atrae la atención de las instituciones castrenses por los resultados que ofrece pues es coherente con los planteamientos de Sun Tzu, en su libro El Arte de la Guerra donde expone: "la mejor victoria es vencer sin combatir"[23]

---

[23] Sun Tzu. El Arte de la Guerra. Página 2.

La ciberguerra en el ámbito militar puede contemplarse como un mecanismo para mantener la seguridad de la información propia y como la implementación de medidas de seguridad para proteger sistemas de comunicación, en especial los empleados para el mando y control en sus diferentes niveles ya que revisten especial importancia para el cumplimiento de las misiones asignadas dentro del marco de operaciones, ya sea para atender situaciones internas como en el caso de Colombia o para asuntos externos cuyo mayor representante es Estados Unidos.

La ciberguerra se convierte actualmente en un facilitador para "conducir operaciones militares como espiar y destruir físicamente los recursos del oponente. Incluye desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadoras, pasando por la planificación de las operaciones, la gestión del abastecimiento, etc.".[24] de manera que durante el desarrollo de las acciones se genera desestabilización y desconfianza de respuesta al emplear estos medios pues no existirá total certeza de su efectividad.

La superioridad en el manejo de la información permite dar aplicabilidad a un nuevo concepto en los principios de la guerra como lo es la opinión pública, casos como la administración de los medios de comunicación pueden generar en la población presión para obligar la toma de decisiones que favorezcan según los intereses que se manejen. De igual forma con un manejo adecuado se puede revertir el pensamiento de una comunidad y que sea ella la que públicamente intervenga y evite acciones de mayor intensidad al verse vulnerada.

Normalmente se toma como primer antecedente formal, de acuerdo a lo conceptuado por la comunidad internacional, el sucedido en Estonia, un país

[24] Sun Tzu. El Arte de la Guerra. Op Cit.

conocido por ser pionero en votaciones por internet y pagos electrónicos de impuestos. A finales del mes de abril de 2007 instituciones como ministerios, medios de comunicación, bancos y en general quienes soportaban en la web su labor, colapsaron por un corto periodo de tiempo al anegarse las redes después de ataques efectuados por parte de unos jóvenes pertenecientes al NASHI, un movimiento juvenil democrático antifascista de Kremlin (Moscú), lugar que solo "abarca un área de 28 hectáreas"[25], que lograron penetrar sitios web apoyados presuntamente desde Rusia. Basado en estos sucesos Vahur Made, de la Academia Diplomática de Estonia iniciando el año 2011 informó:

> "Estonia ha creado una unidad militar de voluntarios informáticos, la Liga de Defensa Cibernética (CDL), con el fin de proteger el país de este tipo de amenazas en el futuro (...) la CDL, forma parte de la Liga paramilitar de Defensa Total de Estonia y, en caso de guerra, estará bajo el mando militar. En la actualidad, está formada por 80 especialistas e ingenieros en tecnología de la información, que se reúnen una vez por semana para practicar simulacros de ataques de piratería informática.[26]

En un mundo altamente tecnificado, las armas no son una excepción. No hay misil que no incluya un ordenador a bordo, y todo el despliegue bélico de cualquier país se decide gracias al poder de cálculo de un puñado de chips. En la actualidad, el mayor exponente de nuestra tecnología es el ordenador. Todos los adelantos en microelectrónica son volcados a la construcción de ordenadores más rápidos y potentes, esto es lo que se está presenciando en estos momentos: la primera guerra de la historia que se produce en un

---

[25] Seyfried, Claus. El Kremlin de Moscú. (en línea) Disponible en http://www.csey.de/rus/kr1_s.htm Consultado el día 26 de septiembre de 2011

[26] Francia. Presseurop.eu. Ciberdefensa Estonia forma un ciber ejército (en línea) http://www.presseurop.eu/es/content/news-brief-cover/462031-estonia-forma-un-ciber-ejercito-modification. Consultado el día 20 de abril de 2011.

entorno virtual pero que tiene victimas muy reales. Desde hace años los gobiernos de los países más desarrollados tienen claro que las guerras del futuro no se desarrollarán en el mundo *offline*, o al menos no en su totalidad.

> "Durante la primera Guerra contra Irak (la Guerra del Golfo), el bando aliado utilizó la tecnología de más alta punta para inhabilitar los dispositivos electrónicos del ejército iraquí, allí se presentaron los primeros cazas y cazabombarderos virtualmente invisibles a los radares convencionales que permitían adentrarse en las líneas enemigas sin ser detectados y eliminar de forma quirúrgica los objetivos enemigos; durante la segunda Guerra de Irak estos sistemas habían evolucionado considerablemente y permitieron a los ejércitos invasores conquistar Irak en pocos días. Los gobiernos que participaron en esta guerra ilegal corrieron para explicar a la opinión pública el éxito de su conquista y el número tan bajo de bajas en combate que habían tenido; pero esto es solo el principio de la nueva concepción del término Guerra Tecnológica que se ha estado gestando en la última década. En paralelo a estos acontecimientos, Internet fue creciendo en número de usuarios e infraestructura tecnológica hasta convertirse en la red neuronal que es hoy en día. Y evidentemente, los gobiernos de varios países Europeos, de Estados Unidos e incluyendo a Irak, saben perfectamente que el nuevo talón de Aquiles está por un lado en la protección de los datos que circulan por Internet y de cómo mantener operativos y a salvo de ataques aquellos servidores gubernamentales y de empresas claves que se encuentran conectados a esta red"[27].

Por otro lado, el gobierno de EEUU y de Cuba, tienen muy claro que Internet está fuera de su control directo y que es un espacio en el que las personas pueden expresar sus ideas y sus opiniones de forma libre y denunciar todas

---

[27] WikiLeaks: La primera ciberguerra de la historia. (en línea) http://oscarpin.com/tag/anonymous/. Consultado el 09 de junio de 2011

aquellas actividades delictivas que realizan tanto las personas como los gobiernos, cosa que como estamos viendo les irrita profundamente[28].

Todo este apoyo informático también puede ser el talón de Aquiles del mejor de los ejércitos. ¿Qué pasaría con las tropas si de repente no funcionase la electrónica que llevan encima? Y más aún: ¿Qué pasaría si se sabotean los ordenadores responsables del funcionamiento de una central nuclear o simplemente de la distribución de energía o las comunicaciones?[29]

Los expertos en seguridad aseguran que los terroristas podrían, utilizando los conocimientos de las vulnerabilidades del software de control utilizado en fábricas, represas o cualquier cosa que imagines, provocar paros, incendios o inundaciones desde el otro extremo de mundo, y a salvo detrás de un "anonimato digital"[30].

Según creen muchos expertos en estos temas, "China ha sondeado en profundidad las redes de datos de los Estados Unidos, preparándose para la ciberguerra"[31]; teniendo en cuenta el último informe del departamento de la defensa de EE.UU., los militares chinos han invertido mucho dinero en crear contramedidas electrónicas y en rubros tales como "ataque a una red de ordenadores", "defensa de una red de ordenadores" y "explotación de una red de ordenadores." Según este informe, el ejército chino cree que este tipo

---

[28] Deisy Francis Mexidor. (en línea). Disponible en http://www.juventudrebelde.cu/cuba/2011-03-21/ciberguerra-mercenarismo-en-la-red/ digital@juventudrebelde.cu. Consultado el 10 de junio de 2011

[29] La guerra que viene. (en línea).Disponible en http://www.neoteo.com/ciberguerra-la-guerra-que-viene. Consultado el 12 de junio de 2011.

[30] CiberGuerra, la guerra que viene (en línea) http://www.pdni.org/2010/09/27/ciberguerra/. Consultado el 12 de junio de 2011.

[31] China, preparándose para una ciberguerra. (en línea) Disponible en http://www.pcworld.com.mx/Articulos/6408.htm. Consultado el 12 de junio de 2011.

de técnicas puede permitir ganar una guerra incluso antes de que comience[32].

Estados Unidos también está desarrollando, desde hace años, estrategias para una eventual ciberguerra; dándole espacio y confiabilidad al "CYBERCOMMAND" recién formado, con el fin de defender los datos, comunicaciones y redes militares, a la vez que están aprendiendo cómo inhabilitar las redes de ordenadores del enemigo y destruir sus bases de datos; y ya fue demostrado que es un caso real, que se ha presentado en las redes principales como lo fue la seguridad de todos los ordenadores de la administración estadounidense, de su ejército y de la NASA, que causo daños por más de un millón de dólares.

La vulnerabilidad de los ordenadores no solo afecta a unos pocos, afecta a todo un estado completo y su sociedad. Nadie está exento de lo que puede llegar a suceder con los llamados simples virus que no se les identifica de la misma manera que se detecta una gripa en el organismo, estos tipos de amenazas virtuales han llegado a causar grandes daños como lo podemos ver en varios casos ya conocidos, como lo fue el de la Otan, y el de Wikileaks.

Habría que decir a los que todavía dudan de la necesidad de ampliar, sin descanso y hasta donde sea posible, la cultura de la seguridad informática que no se puede permitir el lujo de olvidar, ni siquiera por un momento que España tiene el dudoso "honor" de ocupar un lugar destacado en el ranking de los países más atacados por virus, ni que nuestro tejido empresarial está

[32] La guerra que viene. Op. Cit

a años luz de invertir lo necesario en la seguridad TIC para preservar con las máximas garantías el patrimonio de información[33].

Por otro lado el robo de información, en este caso bancaria, está proporcionando suculentos beneficios a los autores de las numerosas estafas por Internet. En España proliferan los correos de phishing, sobre todo los viernes que es cuando más dificultades hay para contactar con la entidad de crédito a fin de hacer la preventiva comprobación. Se ataca a todo desde Internet y que Dios nos libre de que ello afecte a los centros estratégicos, esto sería el caos[34].

La ciberguerra ya es considerada una amenaza real, representantes de la ONU y del mundo corporativo expresaron sus inquietudes en Davos sobre el riesgo que representan los ataques online como disparadores de un conflicto armado. Los ataques contra Google, fueron lanzados desde China según el motor de búsqueda en Internet norteamericano, lo cual represento una discusión del Foro Económico Mundial.

El último informe de McAfee, que recopila información de unas 600 firmas de telecomunicaciones e informática, reveló que el 60 por ciento de los consultados cree que representantes de gobiernos extranjeros están envueltos en operaciones para infiltrar sus estructuras. Asimismo, cerca del 36 por ciento afirmó que Estados Unidos plantea la mayor amenaza, seguido por un 33 por ciento que cita a China[35].

---

[33] Red Seguridad (en línea) http://www.borrmart.es/articulo_redseguridad.php?id=458&numero=17. Consultado el 13 de junio de 2011.

[34] Deisy Francis Mexidor. digital@juventudrebelde.cu (en línea). Disponible en http://www.juventudrebelde.cu/cuba/2011-03-21/ciberguerra-mercenarismo-en-la-red/ Consultado el 13 de junio de 2011.

[35] La ciberguerra se considera una amenaza real. La Nación (en línea) http://www.lanacion.com.ar/1228365-la-ciberguerra-ya-es-considerada-una-amenaza-real Consultado el 13 de junio de 2011

En un mundo que actualmente es dependiente de Internet hasta para manejar la economía, sería razonable pensar que los ataques del futuro no serán contra espacios físicos, sino deshabilitando redes importantes para un negocio, un gobierno o una nación. "*una sola ciberarma podría tener consecuencias globales.*"[36]

La humanidad siempre ha temido por los desastres y la autodestrucción, sin embargo, en estos últimos años parece estar mucho más presente que antes. Y si no se habla del fin del mundo, se habla del fin del mundo como lo conocemos, que es algo muy diferente. Porque eso habla de un enorme cambio y como se dice… todo cambio es bueno. De todos modos, lo que se verá aquí no se presenta como un cambio, sino como una catástrofe y, por eso, NATO se está preparando para una posible ciberguerra.

Ya se ha hablado de que "ciberespías" de varias nacionalidades habían hackeado el sistema de suministro de energía de Estados Unidos y, aunque no hicieron ningún daño, puso al país en alerta. Según NATO, como todo hoy en día sucede a través de Internet, sería lógico que los grandes ataques del futuro (y presente) lo hagan hackers. Es por eso que los mejores especialistas en computación se han reunido en una base militar en Estonia, preparando defensas para una ciberguerra[37].

Por nombrar una de las cosas que están intentando prevenir, se puede mencionar la destrucción de redes de comunicación, que colapsaría el servicio telefónico y de Internet. Y la red de transporte, que produciría una gran amenaza para el tráfico aéreo y ferroviario, además de todos los

---

[36] Artículos destacados. Nato se prepara para una ciberguerra. (en línea) http://www.neoteo.com/nato-se-prepara-para-una-ciberguerra-15578. Consultado el 04 agosto 2011.

[37] Deisy Francis Mexidor. Op. cit.

semáforos en la ciudad. Como se puede ver, una falla en cierta parte del sistema, puede tener muchas repercusiones.

> Aun así, da a pensar lo lejos que ha llegado Internet y lo dependiente que nos hemos convertido de dicha tecnología. A la vez, es cierto que existen riesgos, pero en la vida todo implica un riesgo. Está bien que quieran prevenir algo que tiene posibilidades de suceder, pero tampoco hace falta pintarlo como si fuese tan fácil de lograr y que desembocaría en un apocalipsis cibernético[38].

El Pentágono concluye que los ciberataques son "actos de guerra" y por lo tanto pueden merecer una respuesta militar total Ciberguerra[39]. El primer documento formal de ciberestrategia del Pentágono concluyó que "el sabotaje informático proveniente de otro país puede constituir un acto de guerra", y "abre la puerta para que EE.UU. responda utilizando fuerza militar tradicional"[40].

La mayor parte de las potencias militares establecidas han comprendido el potencial de Internet como campo de batalla y muchos se han estado mojando los dedos en las aguas de la ciberguerra. El primer gusano informático utilizado para infectar servidores de Internet (en 1988) fue creado por un estudiante de posgrado de la Universidad Cornell, cuyo padre era, casualmente, jefe científico del Centro Nacional de Seguridad Informática de la Agencia Nacional de Seguridad de EE.UU.

---

[38] Documentación seguridad. Documentación relacionada con la gerencia de riesgos y los seguros. www.mapfre.com/gerencia-riesgos. (en línea) Disponible en http://www.neoteo.com/nato-se-prepara-para-una-ciberguerra-15578. Consultado el 17 de junio de 2011

[39] identidad Nacional y Natural. (en línea) Disponible en http://identidadlra9.blogspot.com/2011/06/el-pentagono-concluye-que-los.html. Consultado el 05 agosto 2011

[40] Ciberguerra, stuxnet y gente con tejado de vidrio. (en línea). Disponible en http://publicogt.com/2011/06/14/ciberguerra-stuxnet-y-gente-con-tejado-de-vidrio/ Consultado el 17 de junio de 2011

Las reacciones a ese gusano crearon la industria de la seguridad informática como la conocemos en la actualidad, la que por su parte propagó lo que se comienza a conocer como complejo digital militar. **Stuxnet** En julio de 2010, un gusano fue descubierto por una compañía bielorrusa con algunas cargas útiles interesantes. Stuxnet se creó para atacar sistemas SCADA relacionados con centrífugas de gas. El gusano contenía múltiples vectores de ataque que anteriormente se desconocían y que de algunas maneras eran técnicamente sublimes. Este tipo de ciberguerras pueden manejar cifras exageradas de millones de dólares es mucho más económica que el armamento tradicional que habría sido necesario para lograr el mismo resultado[41].

Luego, claro está, se debe ponderar ¿quién sería exactamente el más vulnerable en términos de ciberataques? La respuesta es obviamente: el que está más conectado. La pérdida de acceso a Internet por un día significaría mucho más para Wall Street que para Irán (que bloqueó el acceso a Internet en el pasado)[42].

Ingenieros de sistemas en seguridad de los EEUU, ven esto como el primero de una serie de ataques digitales contra las redes de ordenadores. Casos como el de Estonia o algunos ataques contra las redes del Pentágono no son casos aislados, ni obra de aficionados, de hecho, si los responsables fuesen simples estudiantes que pasan el tiempo en su casa derribando redes de datos de un país como hobby, no generaría realmente una preocupación.

---

[41] El Pentágono concluye que los ciberataques son "actos de guerra" y por lo tanto pueden merecer una respuesta militar total. Ciberguerra, Stuxnet y gente con tejado de vidrio. (en línea)
http://www.rebelion.org/noticia.php?id=130060 consultado el 09 de junio de 2011

[42] Germán Leyens. Rebelión. (en línea) Disponible en http://english.aljazeera.net/indepth/opinion/2011/06/20116673330569900.html. Consultado 17 junio 2011

Dentro de las soluciones que se presentan para una ciberguerra, es difícil que una potencia nuclear denuncie un ataque de este tipo, y menos si ha tenido algún grado de éxito, ya que sería interpretado como una forma de debilidad. Pero dado que todas las armas nucleares de largo alcance están dirigidas por ordenadores, no es imposible tomar el control dirigiéndolas contra su propio dueño u otro país, o al menos inutilizar su sistema de control para convertirlas en chatarra de millones de dólares.

Un ciberconflicto podría tener un impacto enorme, si un enemigo se las ingenia mediante ataques de denegación de servicio para derribar la porción de Internet correspondientes a un país completo. Tanto las emergencias médicas como las comunicaciones de todos los niveles descansan sobre capas montadas sobre internet, incluidas las operaciones financieras, algunos tipos de llamadas telefónicas, etc[43].

Todo esto debería hacernos reflexionar ya que durante años se ha hablado de la locura que significa disponer de millones de megatones listos para ser utilizados en la guerra, pero hoy la tecnología que los controla puede hacer que se transformen en una amenaza real para todo el mundo si logran ser controladas por ciberterroristas. Con el empleo de las Nuevas Tecnologías de la Información y las Comunicaciones (NTIC) y como parte de su estrategia de subversión contra Cuba, el Gobierno de Estados Unidos ensaya en la actualidad una variante de la ciberguerra el fomento de una blogosfera que, aunque se pretende tildar de «independiente», es subordinada de manera total al mandato e intereses de Washington[44].

---

[43] **PDNI – Por la Defensa de Nuestra Identidad**. Ciberguerra, la guerra que viene. (en línea). http://www.pdni.org/2010/09/27/ciberguerra/ consultado el 17 de junio de 2011.

[44] Las razones de Cuba. Ciberguerra, mercenarismo en la red. (en línea). http://www.granma.cubaweb.cu/2011/03/22/nacional/artic05.html. Consultado el 20 de junio 20011

Para los estrategas de la política de Estados Unidos es evidente que quien domine hoy por hoy el ciberespacio tendrá garantizada la hegemonía en lo que han calificado como el nuevo campo de batalla del siglo XXI. No es casual que el antecedente directo de la Internet haya sido Arpanet, una red ideada por el Pentágono para lograr el trasiego de informaciones de sus instituciones militares y de otros centros de investigaciones científicas, lo que evidencia el estrecho vínculo que tuvo la Casa Blanca con un fenómeno asociado al desarrollo de las novedosas tecnologías en el ámbito de las comunicaciones[45].

No se trata ya de que un país, de acuerdo con los postulados actuales tenga un ejército regular con las tres fuerzas tradicionales: mar, aire y tierra, sino de la conformación de un «cuarto ejército», cuyas armas discurren en el escenario virtual de la informática, la computación, las telecomunicaciones[46].

Ciberguerra es una terminología que en la actualidad ronda los escenarios virtuales que desde Estados Unidos se difunden hacia el mundo y específicamente contra Cuba. Las agresiones pasaron a ser desde hace mucho tiempo, embestidas de bytes y redes, una vez que comenzaron a inspeccionar nuestro ciberespacio las 24 horas del día. La humanidad entera ya es además punto de mira del terrorismo mediático y la censura se vierte encima. Hoy las páginas de varios periodistas son clonados en las redes sociales y recientemente se clausuró el canal de Cubadebate en YouTube, supuestamente por la violación del copyright de un video.

---

[45] Ciberguerra: mercenarismo en la red (en línea) **http://rreloj.wordpress.com/2011/03/22/ciberguerra-mercenarismo-en-la-red/**. Consultado el 20 junio 2011

[46] las razones de Cuba. Ciberguerra, mercenarismo en la red. Op. cit

gubernamentales fueron atacadas con el troyano BlackEnergy. Los rusos, considerados autores del ataque, lograron paralizar ciertas páginas gubernamentales. Lo más espectacular fue la toma de control de la web del presidente georgiano, en la que los rusos colocaron durante días fotos de Shalikashvili y de Hitler[49].

Se ha formulado de formas muy diversas la pregunta de si la ciberguerra en realidad existe y quiénes son los que la provocan o emergen en ella, pues según y por definición de Richard A. Clark, experto en el gobierno de los EE. UU. "Existen grupos hostiles alrededor de mundo comandados por Estados o grupos de poder que atacan por razones políticas la infraestructura informática de sus enemigos"[50].

En el 2010 se presentaron singulares ejemplos que sugieren que en Internet se ha estado librando una ciberguerra:

1. Operación Aurora: China vs. Google y otras 20 empresas
2. El virus industrial. Stuxnet Estado-Nación (no identificada) vs. Irán
3. India vs. Pakistán, hackers vulnerando sitios gubernamentales.
4. Estonia tiene una fascinante historia de ciberguerra desde el 2007.

Por otro lado, las acciones defensivas de los EE. UU., no son menores:

1. El Departamento de la Defensa anunció en el 2010 la creación de un nuevo cuartel para su Cibercomando de Fuerzas Armadas (ARFORCYBER)

[49] Guerrillero. Ciberguerra y terrorismo.Op.Cit.
[50] Ciberguerra en dos actos. (en línea) http://alt1040.com/2011/01/. Consultado el 04 agosto 2011

2. La Agencia Nacional de Seguridad (NSA) anunció la creación de un gigantesco centro de ciberseguridad cuyo costo será de 1.500 millones de dólares. El centro de datos se construirá en el Campamento Williams, un centro de formación de la Guardia Nacional de 26 millas al sur de Salt Lake City, que fue elegido por su acceso a energía barata, infraestructura de comunicaciones, y la disponibilidad de espacio, dijo Gaffney. El complejo estará integrado por hasta 1,5 millones de pies cuadrados de espacio construido de 120 a 200 acres, de acuerdo con la filial de la NBC en Salt Lake City[51].

También se ha manifestado como nueva inclusión para el conocimiento de las nuevas arremetidas y preparación ante las posibles amenazas, como ideal para fortalecer y estar atentos a una Ciberguerra como por ejemplo; la intervención del ejército de Corea del Sur como financiador de la creación de un departamento de guerra cibernética en una universidad importante; otro ejemplo es, que los militares también ofrecerán becas completas para 30 estudiantes al año, donde tomarán un curso de cuatro años fuertes en tecnología de la información, la criptografía, la guerra cibernética, psicología y las tácticas de la guerra cibernética, al graduarse los estudiantes becados tendrán que cumplir siete años en el ejército como Cyber especialistas en guerra[52].

CONCEPTUALIZACION DE CIBERTERRORISMO

El ciberterrorismo es la convergencia del ciberespacio y el terrorismo, es "la forma de terrorismo que utiliza las tecnologías de información para intimidar,

---

[51] Informationweek govermment. (en linea). http://www.informationweek.com/news/government/security/221100260. Consultado el 04 de agosto de 2011

[52] Strategy page. (en línea) Disponible en http://www.strategypage.com http://poderiomilitar-jesus.blogspot.com/2011/07/corea-del-sur-crea-la-guerra.html. Consultado el 05 agosto 2011.

coaccionar o para causar daños a grupos sociales con fines políticos-religiosos"[53], esta evolución resulta al cambiar, las armas, las bombas y los misiles por una computadora para realizar y planificar los ataques.

> "A partir de los años 80 la fácil adquisición de computadoras y el acceso a módems telefónicos aumento la vulnerabilidad de los sistemas informativos, lo que permitió el nacimiento de los llamados hackers que son individuos capaces de ingresar ilegalmente en las redes privadas e incluso alterar su contenido, lo cual generó la posibilidad de que un grupo terrorista pudiera cometer atentados o sabotajes mediante el empleo de medios telemáticos desde cualquier lugar del mundo, dando origen al termino ciberterrorismo".[54]

Nos encontramos en la actualidad con un panorama diverso que nos permite afrontar y confrontar con las diferentes "caracterizaciones" de los delincuentes informáticos, hablamos de hacerks, crackers, phreackers y los casos más preocupantes, los "ciberterroristas".[55]

Según la definición oficial del FBI, "el terrorismo es el uso ilegal de la fuerza o la violencia contra personas o propiedades a fin de intimidar o cohesionar al gobierno, la población civil o cualquier otro segmento, persiguiendo objetivos sociales o políticos". El Departamento de Estado norteamericano define, "El término terrorismo implica actos de violencia premeditada y políticamente

---

[53] GASCO Leandro, La Ciberbatalla y los gobiernos destructores de instituciones (en línea) Disponible en http://www.radiomiami.us/noticia.php?idn=5615 Consultado el 04 de agosto de 2011

[54] MASANA Sebastián, El ciberterrorismo: ¿una amenaza real para la paz mundial? (en línea) Disponible en http://www.argentina-rree.com/documentos/ciberterrorismo.pdf Consultado el 05 de agosto de 2011

[55] SALELLAS Luciano, Delito informático y ciberterrorismo (en línea) Disponible en http://www.forodeseguridad.com/artic/discipl/4075.htm Consultado el 04 de agosto de 2011

motivada perpetrados contra objetivos no combatientes por grupos subnacionales o agentes clandestinos".[56]

Según Barry Collin, un investigador sénior del Institute for Security and Intelligence en California "ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos" [57]

Durante los años 90 con la masiva penetración del internet en la sociedad se aumentó la hipótesis de los ataques ciberterroristas, fomentándose la proliferación de hackers debido a lo sencillo que es penetrar una red o crear virus capaces de infectar miles de computadoras, lo que generó en los medios de comunicación, desinformación masiva y exagerada sobre las capacidades y el accionar de los hackers, para lo cual se adoptan medidas preventivas en relación al ciberterrorismo durante la administración de Bill Clinton.

En 1984, el escritor de ciencia ficción William Gibson acuñó el término ciberespacio (cyberspace) en su novela Neuromante donde ciberespacio se refiere a una vasta matriz de datos controlada por poderosas compañías, la matriz de Gibson tiene una interfaz visual y tridimensional, que permite a los

---

[56] Terrorismo.com. Las definiciones del FBI y el Departamento de Estado (en línea) Disponible en http:// www.terrorismo.com. Consultado el 05 de agosto de 2011

[57] Declaraciones de Barry Collin: Disponible en http://www.af.mil/news/Feb1998/n19980206_980156.html Consultado el 05 de agosto de 2011

usuarios navegar luego de "enchufarse" (jacking in) o conectarse a través de equipos especiales.[58]

> El ciberespacio es un lugar virtual de bits y bytes, en oposición al espacio físico de átomos y moléculas, se refiere a un entorno no físico creado por equipos de cómputo unidos para inter operar en una red, en el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir, la información se puede intercambiar en tiempo real o en tiempo diferido y la gente puede comprar, compartir, explorar, investigar, trabajar o jugar. "La Internet constituye el mayor ámbito del ciberespacio".[59]

"Desde el momento en que gran parte de nuestra actividad se desarrolla digitalmente (desde las transacciones bancarias hasta la compra y venta de acciones en las bolsas) es útil tener una expresión que permita a todo eso formar parte de un territorio", expresó el mismo Gibson[60].

Durante la última década las intrusiones e incidentes de seguridad han crecido de manera exponencial estableciendo un escenario oscuro sobre la seguridad de las infraestructuras de computación en el mundo. Los organismos han adelantado en sus análisis de seguridad, instalando

---

[58] MASANA Sebastián, El ciberterrorismo: ¿una amenaza real para la paz mundial? (en línea) Disponible en http://www.argentina-rree.com/documentos/ciberterrorismo.pdf Consultado el 06 de agosto de 2011

[59] INTERFICTO, ¿Qué es el Ciberespacio? (en línea) Disponible en www.articulo.org/articulo/25407/que_es_el_ciberespacio.html Consultado el 04 de agosto de 2011

[60] Entrevista televisiva realizada en Suecia para el programa televisivo Rapport, noviembre 3, 1994. El audio de la entrevista completa (en inglés) (en línea) Disponible en http://www.josefsson.net/gibson/ Consultado el 07 de agosto de 2011

múltiples mecanismos de protección y efectuando múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de trabajo.

> "Dorothy E. Denning directora del Georgetown Institute for Information Assurance de la Georgetown University califica como ciberterrorismo, un ataque o ataques que debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo, que deriven en muertes o personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas al afectar la infraestructura crítica de un país podrían ser considerados actos de ciberterrorismo", dependiendo de su impacto.[61]

El objeto de un ataque ciberterroristas no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general.

El ciberterrorismo existe porque engloba tanto la utilización de las TIC y más concretamente Internet como elemento de apoyo a la infraestructura de sus organizaciones (comunicaciones, apología y propaganda, reclutamiento, financiación, etc.) y como objetivo de la acción directa (ataques informáticos contra objetivos tecnológicos tales como operadores de telecomunicaciones, infraestructuras críticas, etc.).

Ante la cuestión de si se ha materializado de alguna manera la amenaza ciberterrorista, las organizaciones terroristas vienen aprovechando las

---

[61] CIBERTERRORISMO, Una Amenaza gubernamental a la privacidad (en línea) Disponible en http://www.paginasprodigy.com/tesisdehackers/cibercap1.html Consultado el 04 de agosto de 2011.

posibilidades que les ofrecen las TIC en su propio reino cibernético donde son más débiles la mayoría de las naciones industrializadas. El terrorismo existe en nuestro mundo real, y con todos los avances tecnológicos era lógico que pronto usasen los medios virtuales para generar sus ataques terroristas. Comienzan con la captación de Ciberpiratas, chequeando sus visitas a cierto tipo de webs, haciendo un rastreo en la participación de ciertos foros y si todo esto les convence por perseguir ciertos ideales afines, son captados para pertenecer a su grupo de ciberterroristas.

Se comunican entre ellos usando" la ESTEGANOGRAFÍA, que es un método que permite la ocultación de ficheros de audio, vídeo, texto y gráficos, camuflándolos de la sabida monitorización de los Ciberespías, y se usan en correos electrónicos, en chat y en teléfonos móviles y vídeo conferencias encriptados."[62]

Su financiación económica, la consiguen con la extorsión a grandes empresas o entidades, con las amenazas de un ataque o revelación de datos de clientes o secretos empresariales, obteniendo así suculentas subvenciones que muchas veces camuflan a través de entidades benéficas para blanquear el dinero, tanto por parte del que lo da, como del que lo recibe.

¿Cómo se publicitan?, generalmente "se apropian de varias webs, sobre todo empresariales para publicar sus atentados, y en pocos segundos sus mensajes terroristas son difundidos por todo el planeta, sus objetivos son paralizar la capacidad militar y el servicio público de un país y pueden

---

[62] SENOVILLA, Ciberterroristas, (en línea) Disponible en http://www.vinagreasesino.com/articulos/ciberterroristas.php Consultado el 07 de agosto de 2011

comenzar con ataques a los mercados financieros, para continuar con un ataque a los sistemas informáticos gubernamentales."[63]

Su modus operandi comienza con la explotación cuyo objetivo es obtener información y recursos del destinatario, siguen con el engaño que consiste en manipular esa información obtenida pero permitiendo operatividad al destinatario y finaliza con la destrucción, que es cuando ya dejan inoperante al destinatario, destruyendo todos sus sistemas; aunque algunas veces, esta inoperancia es temporal para aprovechar sus recursos.[64]

A nivel mundial los países están preocupados por el ciberterrorismo y por esto mismo existen dos tendencias: los que apoyan la conformación de una "ciberpolicía" que trascienda las fronteras y los que se inclinan a favor de mejorar la cooperación internacional. La cibernética e Internet son un campo muy fácil de abordar para los dos bandos.

Debemos estar muy alertas a este nuevo tipo de guerra y terrorismo, debido a que la civilización de tipo occidental se apoya en un grado mucho más alto en la tecnología basada en computación y redes, por lo que Internet es un trampolín y base para que los terroristas puedan concebir, planear, tener logística y ejecutar futuros ataques.

El ciberterrorismo requiere de un alto entrenamiento y gran dedicación, pero como es difícil de rastrear y el daño al "enemigo" puede ser desde considerable hasta muy grave, debemos establecer una continua

---

[63] SENOVILLA, Ciberterroristas, Op.Cit

[64] Ibid.

cooperación en materia de seguridad, manejo de crisis y tecnología avanzada en la lucha contra el terrorismo a nivel mundial.[65]

CONCEPTUALIZACIÓN DE LA CIBERDEFENSA

Se ha presentado que no solo en Colombia, sino en muchos países del mundo entero el diario vivir de ataques cibernéticos, decadencias por fuga de información y fallas en la seguridad de la web, ha generado una gran serie de problemas y desestabilizaciones sistemáticas, es así como la Ciberdefensa entra a realizar un rol muy importante para detectar invasiones y ataques dentro de la web, accionando alarmas y actuando de manera eficiente ante este tipo de terrorismo.

Tras la cantidad de filtraciones, amenazas y ataques que se han presentado por manipulación de la información en la web, tanto en el sector público como en el privado, saltando todo tipo de seguridad en la tecnología, es de argumentar que estamos atravesando una nueva tendencia de riesgos que pueden llegar a afectar tanto directa como indirectamente la funcionalidad de una organización o de un país.

La Ciberdefensa debe mantener una infraestructura de acción ante el conocimiento de información crítica, que puedan llegar a afectar la gobernabilidad de la nación. En este caso la seguridad cibernética de un país debe cuidar los sectores más importantes para el bienestar de este, que son: la energía eléctrica, producción, almacenamiento y suministro de gas, petróleo, telecomunicaciones, bancos y finanzas, suministro de agua,

---

[65] SALELLAS Luciano, Delito Informático o Ciberterrorismo (en línea), Disponible en http://forodeseguridad.com/artic/discipl/4075.htm Consultado el 07 de agosto de 2011

transporte, servicios de emergencia y operaciones gubernamentales (mínimas requeridas para atender al público), la afección de alguna de estas pondría en riesgo la funcionalidad de una nación y se prestaría para que la ciudadanía pierda confianza al gobierno por no actuar eficazmente ante este tipo de amenazas.

Como resultado de esto se puede decir que el término de Ciberdefensa es una respuesta a las diferentes amenazas y ataques provenientes de la ciberguerra o del ciberterrorismo, esa nueva relación regular e invariable que deben desarrollar todos los gobiernos para comprender ahora sus responsabilidades de Estado, en el contexto de un ciudadano y fronteras nacionales electrónicas o digitales.

Un concepto estratégico de los gobiernos que requiere la comprensión de variables entre otras, la vulnerabilidades en la infraestructura crítica de una nación, las garantías y derechos de los ciudadanos en el mundo online, la renovación de la administración de justicia en el entorno digital y le evolución de la inseguridad de la información en el contexto tecnológico y operacional[66].

Considerando lo anterior, las reflexiones y decisiones sobre la seguridad nacional, tienen una renovada connotación, para atender ahora un enemigo móvil, cambiante y evolucionado que se mueve tanto en las infraestructuras críticas como fuera de ellas, que tiene claro y sabe lo reactivo que son las empresas y gobiernos, y que aun así se pueda ser identificado en sus ataques, se hace poco creíble probar que existió.

---

[66] ITU (2010) Global cybersecurity agenda. (en línea) Disponible en http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf Consultado el 15 de abril de 2011.

La defensa nacional, como misión encomendada a las Fuerza Militares del país, requiere ser analizado en el contexto de la nueva forma de la guerra, de una confrontación que enfrenta lo mejor de los entrenados en la forma de la inseguridad de la información, con lo mejor de los entrenados para controlar la seguridad informática y mantener la paz de una nación. Por lo tanto, se debe animar una revisión de las estrategias de seguridad nacional en el sentido de evitar posibles y factibles escenarios de confrontación tecnológica y de guerra de la información.

A la fecha muchos estados han tomado acciones concretas frente al reto de la Ciberdefensa, encontrando en sus ciudadanos los primeros y más importantes aliados en sus estrategias de protección de la nación en el contexto digital. Dichos estados comprenden que es, desde el ciudadano y su experiencia en el uso de las tecnologías de información y comunicaciones, donde puede fortalecer el perímetro extendido de seguridad nacional digital, aunque sabiendo que es poroso y poco confiable, sabe que allí encuentra su mejor carta para hacer realidad su visión de defensa de la nación en un mundo interconectado[67].

Para darle vida a esta visión de la defensa nacional digital, se requieren elementos específicos que materialicen ese querer en acciones detalladas, que aplicadas en las tecnologías de información e interiorizadas en los hábitos de los ciudadanos, puedan hacer evidente esa nueva propiedad naciente denominada seguridad nacional digital, esa que genera confianza, respeto y confiabilidad en las iniciativas del gobierno frente a la realidad de la creciente dinámica informática y de las telecomunicaciones.

---

[67] ITU (2010) Global cybersecurity agenda. Op. Cit

Considerando lo anterior, se hace evidente que los gobiernos, no pueden hacer realidad su nueva visión de la defensa, sin una estrategia concreta de prácticas de seguridad de la información, como base fundamental de su visión de seguridad nacional, donde cada uno de los individuos reconozcan en la información ese activo fundamental que articula todas las infraestructuras críticas de la nación.

De esta manera el concepto de ciberseguridad, como realidad complementaria de la Ciberdefensa materializa el concepto de defensa nacional, en un conjunto de variables claves acertadamente definidas por la ITU – International Telecommunication Unión, en las cuales se hacen necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación en el contexto de una realidad digital y de información instantánea[68].

La ITU, entendiendo que la problemática de la ciberseguridad requiere un esfuerzo colectivo y coordinado entre los diferentes países; establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional[69].

Si vemos cada una de las variables establecidas por la ITU, no buscan otra cosa que comprender los riesgos propios de una sociedad de la información

---

[68] Ciber seguridad y ciber defensa: Dos conceptos emergentes en la gobernabilidad de una nación. Detallando las prácticas de aseguramiento. (en línea). http://www.belt.es/articulos/HOME2_articulo.asp?id=8387. Consultado el 16 de abril de 2011.

[69] Ibid.

digital y en constante movimiento, que considere los aspectos normativos, las tecnologías de seguridad de la información, la organización de la seguridad de la información necesaria para operar, la cultura de seguridad de la información y la cooperación entre países, como fuente de la armonización de visión de la ciber seguridad en el planeta[70].

La OTAN articula sus decisiones a través de los siguientes organismos internos:

El Consejo del Atlántico Norte – el comité político de decisión al más alto nivel – tiene el control total sobre las políticas y actividades relativas a Ciberdefensa. El Comité de Planeamiento y Política de Defensa – DPPC, ha desarrollado las propuestas a nivel político (es decir, preparación de una política de Ciberdefensa y decisión OTAN sobre la creación de la Autoridad de Gestión de Ciberdefensa) para la aprobación por el Consejo[71].

El Comité de Consulta, Mando y Control - NC3 constituye el organismo principal de consulta de los aspectos técnicos y de implementación sobre Ciberdefensa. Las Autoridades Militares - NMA y la Agencia de Consulta, Mando y Control - NC3A que tienen la responsabilidad de identificar los requisitos operacionales y la adquisición e implementación de las capacidades de Ciberdefensa[72].

---

[70] CANO, J. (2008) La guerra fría electrónica y la inseguridad de la información. Publicación en Blog. (en línea) Disponible en http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=450012245&random=4197 consultado el 15 de abril de 2011.

[71] DOCUMENTO INFORMATIVO DEL IEEE 09/2011. NUEVO CONCEPTO DE CIBERDEFENSA DE LA OTAN. (en línea). http://www.belt.es/expertos/imagenes/DIEEEI09_2011ConceptoCiberdefensaOTAN.pdf. Consultado el 18 de marzo de 2011.

[72] Documento informativo del ieee 09/2011, Nuevo concepto de Ciberdefensa de la OTAN (marzo de 2011).

Es de mucha importancia conocer que se está haciendo ante este nuevo tipo de guerra, ya que a raíz de las nuevas tendencias nos vamos arraigando más a los medios tecnológicos que permiten llevar y traer todo tipo de información en la que emerge nuestra vida cotidiana.

La ciberdefensa debe estar actuando continuamente y creando estrategias de ejecución para eventualidades de ataques, a fin de proteger y estabilizar de manera efectiva la infraestructura de los sistemas operacionales que hacen dar viabilidad al funcionamiento de nuestro país y al bien propio.

Siguiendo la información y el concepto de ciberdefensa, se conoce que se han realizado acciones y estudios que permitan adelantar logros ante la problemática de Ciberterrorismo, una amenaza vigente en el círculo digital, en el mundo cibernético que estamos viviendo y del cual estamos convirtiendo como esencial para la cotidianidad, sin tener en cuenta que ante nosotros mismos recae una gran responsabilidad y no solo a la seguridad del estado.

Es de saber que esta es una guerra a la que se le debe dar mucha importancia, ya que puede afectar la integridad de nuestro país y se debe accionar prestándole la atención inmediata que se requiere para llegar a los directos agresores o terroristas, cabezas de las bandas delincuenciales que pretenden dañar el bienestar de una nación que ahora se mueve digitalmente.

EMPLEOS DE LA GUERRA DE REDES

TECNICAS INFORMATICAS

El Avance tecnológico de la época en que se vive se sabe que los Ejércitos de todo el orbe usan elementos sofisticados de empleo para la conducción estratégica y táctica para la administración de personal y medios frente a los Estados modernos, con organizaciones muy complejas, en donde la comunicación instantánea en todo el mundo entre las fuerzas aéreas, marítimas y terrestres es fundamental para las operaciones militares[73].

La capacidad de los militares en las operaciones de información incluyen la guerra en técnicas de información y comunicación en las operaciones militares, las desinformación militar y la seguridad de operaciones, son debidamente coordinadas y estrechamente concentradas, estas capacidades pueden disuadir el conflicto,

Al hablar de seguridad y defensa nacional nos encontramos con un factor que trasciende las fronteras y es la base legal que garantiza que los Estados tengan las herramientas necesarias para poder emplear a las instituciones armadas, los organismos de seguridad pública y los organismos de inteligencia del estado el cual juegan un papel muy importante en el manejo de la información de las amenazas crecientes.

De esta forma, las operaciones militares, o la Fuerza de Tarea, cuentan rápidamente con ganar cualquier enfrentamiento cinético, desde el comienzo, para llevar a cabo las operaciones de información con la misma capacidad y un desarrollo constante que si bien está favoreciendo a las sociedades de nuestro hemisferio, también se convierten en una amenaza; la tecnología juega un papel importante, no es por sí sola, de utilidad sino tiene que ir ligada a los medios tecnológicos utilizados por una nación, de un

---

[73] Reig, Ramón (1995): El control de los medios de comunicación de masas: bases estructurales y psicosociales

conglomerado para que pueda garantizar su progreso, de prosperidad, seguridad y bienestar, pueden ser utilizados para bien de la nación[74].

En este orden de ideas, las redes informáticas contra una red de comunicaciones del Estado puede impedir, deteriorar o interrumpir su uso para fines de mano y control de las fuerzas militares, o su uso por parte de los líderes claves a fin de coordinar una respuesta nacional.

ORIGEN DE LAS TECNICAS INFORMATICAS EN LAS OPERACIONES MILITARES

Cuando comenzó la Segunda Guerra Mundial, había un pequeño grupo de investigadores militares, encabezados por A.P. Rowe, interesados en el uso militar de una técnica conocida como radio-ubicación (o radio-localización), que desarrollaron científicos civiles. Algunos historiadores consideran que esta investigación es el punto inicial de la investigación de operaciones.

Esta consiste en enviar información que influya o disuada a los líderes adversarios claves y sus estructuras de apoyo de manera que impida las subsecuentes medidas adversas por parte del adversario. Las operaciones de apoyo de información militar son eficazmente empleadas como una capacidad integrada de las operaciones de información en apoyo.

Las Técnicas Informáticas en las operaciones militares, pueden disuadir el conflicto armado tanto con posibles adversarios estatales como los no estatales, la habilidad de justificar el uso de las operaciones de información de ofensiva como algo prudente, desde el punto de vista moral, contribuirá,

---

[74] APPLEGALE MELISA, Informe publicado sobre Ciencia y Tecnología publicado por El Stralegre Studies Institute, septiembre de 2001.

considerablemente, a que la comunidad internacional acepte el uso de las operaciones de información no constituye el uso de la fuerza en el sentido tradicional.

Las capacidades militares básicas de las operaciones de información incluyen la guerra electrónica, las operaciones de redes informáticas, las operaciones de apoyo de información militar, las operaciones de des-información militar y la seguridad de operaciones. Las cuales son debidamente coordinadas y estrechamente concentradas, estas capacidades pueden disuadir el conflicto armado.

Los medios tecnológicos y la gestión de información generan un nuevo conocimiento jugando un papel prioritario en el éxito o el fracaso de las actuaciones de las fuerzas y cuerpos de seguridad del estado, en el ámbito de la prevención por medio de la información.

Paralelamente, la incautación de documentación generada por la actividad logística de un comando terrorista en forma de discos duros, memorias, ópticas, libros contables, correspondencia y publicaciones, etc., originan un nuevo enlace y de avanzada hacia la vía de investigación.

Sin lugar a dudas, el avance tecnológico se ha presentado en forma significativa, y sobre todo en el campo de batalla moderno, el cual se ha visto influenciado por el acelerado ritmo de las operaciones, en que la función de Inteligencia tiene que interactuar con modernas tecnologías para cumplir su misión[75].

---

[75] MATAMALA APARICIO Salvador, Guerra de la Informática, monografías Chile 13 de enero de 2009.

Además, de esa obtención de información, procesarla y difundirla son las etapas en que se presenta la necesidad de incorporar los equipos y software, estos equipos de comunicaciones van en ayuda de la misión que cumplen las tropas de información, que se relacionan activamente con toda la fuerza de una operación bélica, y sobre todo en el ámbito y conjunto en todos los niveles de la conducción militar.

El empleo de adelantos tecnológicos como apoyo al avance de la humanidad, especialmente en el campo estatal, militar y científico ha permitido alcanzar nuevos horizontes que facilitan el alcance y cumplimiento de los objetivos e intereses de las diferentes naciones que se soportan en tecnologías para interactuar con el mundo entero. Lo anterior ha creado puntos tanto de vulnerabilidad como de fortalezas para el normal funcionamiento de la institucionalidad de los países, que de acuerdo a su presupuesto realizan inversiones en seguridad informática para evitar ataques y filtraciones especialmente en el campo bélico puesto que es el que les garantiza seguridad y progreso.

Los diferentes Estados a nivel global en su mayoría emplean las Fuerzas Armadas para garantizar su soberanía e intereses, por lo tanto propenden dotarlas de los equipos necesarios para el cumplimiento de su misión, y, coherentes con los cambios buscan mantener equipamiento con tecnologías de punta de manera que se les garantice los mayores índices de seguridad durante su empleo. Con el pasar del tiempo son menos viables los enfrentamientos directos entre ejércitos, especialmente entre potencias, hoy en día aumentan las tendencias por medios que no pongan en riesgo la integridad humana ocasionando que las contrapartes desarrollen habilidades que no impliquen la difusión de su identidad y origen.

El término de guerra de red es empleado inicialmente por el politólogo David Ronfeldt, un norteamericano que desarrolló proyectos de investigación para el Pentágono por conflictos desarrollados en México y un grupo revolucionario de ese país llamado Ejército Zapatista de Liberación Nacional el cual empleaba lo que en su momento lo llamaron como una guerra socio informática constituyendo uniones o coaliciones internacionales para que coordinadamente atacaran al gobierno mexicano en sus redes sociales.

> "Las batallas de la guerra en red no enfrentan a ejércitos, y sus combatientes son grupos terroristas como Al Qaeda y militantes anarquistas como el Black Bloc. También lo son los ecologistas o los activistas de la sociedad civil que luchan por la democracia y los derechos humanos. Pero todos ellos tienen en común que presentan formas de organización en red y operan en pequeñas unidades dispersas que se despliegan con rapidez en cualquier lugar y en cualquier momento. Desde las redes de terroristas y delincuentes hasta la Batalla de Seattle y el movimiento zapatista, (...) Aunque los terroristas continúan poniendo en peligro la seguridad norteamericana y europea, a largo plazo —sostienen John Arquilla y David Ronfeldt en el prólogo a la edición española del libro la aparición de una sociedad civil global estructurada en red supondrá un fenómeno más poderoso, duradero y transformador"[76]

Con la sencilla circulación de un mensaje apoyado en otras redes con la misma idea pero con diferente presentación se logra influir en masas suficientes que se encargan de diseminar aun mas estos correos por otros medios y redes haciendo

[76] Arquilla, John. Y Ronfeldt, David. Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político. (en línea) Disponible en: http://dialnet.unirioja.es/servlet/libro?codigo=232687 consultado el 19 de junio de 2011.

que llegue a una mayor cantidad de gente, que a su vez "(...) generan empatías con mensajes que resultan sensibles a un sector social con miras a movilizarlos y hacerlos presentes en las redes sociales. Una vez que se logran los 'umbrales de rebeldía' se los organiza en comunidades virtuales, grupos sectorizados, asociaciones de distintas índoles que proyecten un activismo desaforado que compense en acción lo que no se tiene en respaldo político real".[77]

Las redes se pueden presentar bajo tres tipos básicos que son:[78]

- **Cadena:** las organizaciones, personas, mercancías e información se mueven a lo largo de una línea separada por diferentes nodos que interconectan toda la línea.

- **Estrella:** existe un nodo, que puede ser uno o varios actores, que actúa como centro no jerárquico, comunicando y coordinando a los otros nodos de la red.

- **Multicanal:** en este caso todos los nodos y los actores que conforman éstos en la red están conectados entre sí.

Un gran poder de opinión pública se logra en otras acciones abiertas como la evidenciada en Colombia que promovió una movilización por internet, en contra del mayor enemigo de ese país: el narcoterrorismo, donde multitudes acudieron al llamado por la paz y llenaron varias calles del país y de las principales ciudades del mundo. Respecto a empleo de medios a través de tecnologías, es reconocido por

---

[77] Agencia Latinoamericana de Información. Facebook y Twitter: trincheras de la netwar (en línea). Disponible en http://alainet.org/active/36476&lang=es consultado el día 19 de junio de 2011.

[78] Arquilla, J. y Ronfeldt, D. (1996), El advenimiento de la guerra red, California, RAND Corporation, p. 22. Publicado por la Universidad Javeriana - Colombia. Forigua Rojas, Emersson. (2006) LAS NUEVAS GUERRAS: UN ENFOQUE DESDE LAS ESTRUCTURAS ORGANIZACIONALES (en línea) Disponible en http://www.javeriana.edu.co/politicas/publicaciones/documents/9LASNUEVAS.pdf consultado el día 20 de junio de 2011.

potencias y personalidades de renombre mundial quienes se han manifestado públicamente conceptos como por ejemplo:

> "Como hemos visto en Túnez y Egipto, el genio se ha salido de la lámpara. Las tecnologías de la conexión están por todas partes y se propagan rápidamente, y le han dado a la gente herramientas poderosas para imaginar un mejor futuro para sí mismos y luego hallar aliados que les ayuden a lograrlo. Esto ha amplificado los llamamientos a la democracia, que aumentan a medida que Internet se propaga, y suprimir esos llamamientos sin acudir a medidas extremas sólo será más difícil para los gobiernos".[79]

El impacto y la fuerza de la opinión pública puede dar vuelcos a situaciones que se presentan como desfavorables si ellos no están de acuerdo y retiran su apoyo para continuarlas, como el caso de Estados Unidos con Vietnam y recientemente con los cuestionamientos que le hacen al gobierno norteamericano por involucrarse en situaciones del Medio Oriente pues están reclamando el por qué de la intervención y los sacrificios en vidas, heridos y presupuesto. Para la guerra de red puede también emplearse medios basados en software y programas, también influye la guerra mediática influenciada por las redes sociales que coadyuvan a golpear contundentemente a naciones sin efectuar un solo disparo.

Aún así, Los Estados unidos en su lucha contra el terrorismo internacional, tenía dentro de sus objetivos el neutralizar a Osama Ben Laden y la red que lideraba, pero para poder derrotarlo era consciente de la necesidad de emplear las redes. Según John Arquilla docente y ex miembro de las Fuerzas Armadas de Norteamérica, opina al respecto:

---

[79] Embajada de los Estados Unidos en Bogotá. Apartes del Discurso de la Secretaria de Estado Hillary Clinton sobre Libertad en Internet (en línea). Disponible en http://spanish.bogota.usembassy.gov/pr_018_15022011.html consultado el día 19 de junio de 2011.

> En la Netwar, "gana el que tiene la mejor información, no el que tiene la bomba más grande". El resultado de los conflictos depende cada vez más de la información y de las comunicaciones, lo que facilita la flexibilidad y tiende a "favorecer las organizaciones en red frente a las jerarquías" de los ejércitos tradicionales. Arquilla estima que actualmente "el 90% de nuestros esfuerzos están constituidos por estrategias militares contra Estados (state actors)". Ello refleja un pensamiento militar arcaico, que data de la amenaza soviética y "que no permite responder a las necesidades de una guerra contra una red". Se trata además de una solución facilista, explica: "Es más o menos como si, al no saber qué hacer, hiciéramos lo que sabemos hacer. Sabemos cómo comportarnos frente a los Estados-nación, pero no sabemos bien qué actitud adoptar frente a las redes".[80]

Los cambios y actualización de las doctrinas se modifican y ajustan acorde a la evolución de los conflictos y a las formas de operar que permiten los diferentes avances tecnológicos a nivel mundial. Ante esto es importante que las naciones no se olviden de sus principios y valores, y como en el caso planteado en el párrafo anterior, hacer las cosas que mejor se saben hacer puesto que dentro de la legalidad de las normas internacionales se ha demostrado que pueden obtenerse excelentes resultados sin desligarse de la doctrina operacional y la guerra regular que es la principal razón de ser de los ejércitos.

La complejidad de acertar en la designación de los objetivos militares puede ocasionar que estas redes se desplazan a lugares donde podrían nunca ser ubicados, antecedentes como en el que "Al-Qaeda perfeccionó enormemente el arte de establecer contactos con otros grupos y de ayudarlos a establecer lazos entre

---

[80] Pisani, Francis. Le Mondé Diplomatique (El mundo Diplomático) Edición Cono Sur. Nueva guerra contra nuevo enemigo. Número 36 - Junio 2002, páginas 10-11

ellos (...), a poner en contacto a individuos de un grupo con los de otro grupo para realizar ciertas operaciones precisas"[81] dan muestra de la facilidad que tienen para diseminarse y mantener un contacto que fortalece las organizaciones y su clandestinidad de su actuar rearticulandose constantemente agregando o reemplazando nuevos nodos.

Este tipo de guerra de red es una forma de reaccionar ante un poderío bélico que difícilmente se pueda igualar o superar y que sumado a un incompetente manejo de medios ocasiona un fortalecimiento de imagen de quienes vulneran las capacidades estatales al colocar en tela de juicio la competitividad y eficiencia de sus aparatos armados y de inteligencia ante una a incursión invisible en un territorio deslocalizado de sus objetivos generalmente móviles, diseminados y oportunistas que están en un momento ubicados en un lugar y en cualquier momento se cambian a otro, atravesando fronteras de manera casi invisible.

La guerra de red se enmarca dentro de resultados perturbadores modificando ostensiblemente los teatros de operaciones tradicionales sin un inicio o final determinado dependiendo de la eficacia de la capacidad de comunicación y efectos de desestabilización. Adicionalmente y "(...) como ocurre a menudo con los ejércitos– no han sabido adaptarse como debían a las distintas circunstancias y han descubierto a las malas que sus enemigos, muchas veces, les llevan la delantera"[82] ocasionando algunas pérdidas humanas y en gran medida financieras al no vislumbrar los cambios de los conflictos.

"El mayor problema que afrontan hoy los ejércitos tradicionales es que están organizados para librar grandes guerras y les resulta difícil orientarse hacia otras más pequeñas"[83] corroborando con ello que si los ejércitos de cualquier país no

---

[81] Pisani, Francis. Le Mondé Diplomatique. Op. Cit.

[82] Uruguay. Revista La Onda Digital. Artículo de Arquilla, John. También los que hacen las guerras, ahora piensan en la Redes (en línea). Disponible en http://www.laondadigital.com/laonda/laonda/478/B1.htm consultado el día 27 de 2011.

[83] Ibíd.

avanzan a la par de los cambios son los mismos países los que saldrían perjudicados y sus contrincantes serian los mayores beneficiados de esta imposibilidad de romper paradigmas al sostener una mentalidad de que la masa y los equipos bélicos más sofisticados podrán vencer estas estructuras de grupos o estados interesados en desestabilizar la política de un país.

Es limitada la experiencia con que cuentan los ejércitos para enfrentar situaciones de guerra a través de las redes, pero no solo deben limitarse a salvaguardar la soberanía en tierra, mar y aire, es imperativo que dediquen esfuerzos no solo para abarcar el espacio en sus tres dimensiones, sino también el ciberespacio aunque sus capacidades estén limitadas por normatividades internacionales existentes y que les permitan neutralizar el empleo de maquinaria, equipos, sistemas de suministros, comunicaciones, sistemas de mando y control mediante la infiltración y reprogramación

LAS TIC'S EN OPERACIONES MILITARES DE ALTO RIESGO EN COLOMBIA

Los cambios producidos en las formas y la conducción de los conflictos armados comprende estrategias en las " ***Técnicas informáticas y comunicación en las Operaciones Militares***" , el amplio espectro, comprende estrategias, no tradicionales e inquietantes desde el punto de vista de la política y de la conducción de la seguridad del estado , como una situación de garantía y tranquilidad propiciada por el poder nacional, para poder alcanzar y mantener los objetivos nacionales como lo es preservar, la soberanía, progreso, bienestar teniendo en cuenta los límites y funciones de los miembros de la Fuerza Pública, tienen entre otros para la defensa y seguridad del Estado y de conformidad a lo establecido por la Constitución y la Ley son:

FUNCIONES DEL EJÉRCITO

Al Ejército le corresponde la defensa terrestre y tendrá además las siguientes funciones:

1. Organizar, equipar y adiestrar unidades para la ejecución de operaciones militares terrestres.
2. Establecer la doctrina y los procedimientos para la ejecución de la guerra terrestre y su participación en operaciones aerotransportadas o de orden público que sean de su competencia.
3. Participar en la ejecución de los planes de movilización militar.
4. Mantener la integridad de las fronteras terrestres y contribuir a su desarrollo.
5. Realizar actividades de investigación y desarrollo en áreas científicas y técnicas dirigidas a fortalecer la defensa nacional.
6. Las demás que se señalen en las leyes y reglamentos.

CREACIÓN DE LA DIRECCIÓN DE INFORMÁTICA MILITAR

El Centro de Informática Militar empezó su funcionamiento a partir del 18 de Agosto del año 1980, y como base se encontraba en la Corporación de la Fuerzas Armadas de la Nación (COFADENA), que se encuentra ubicada en la Av. 6 de Agosto, donde realizaban diferentes trabajos concernientes a la Administración de Personal, cumpliendo los requerimientos del Departamento I- EMGE.

A partir de la gestión 1982, el Centro de Informática Militar pasa a depender directamente del Comando General del Ejército, la misma que empieza a funcionar con una Sección de Procesamiento y Automatización de Datos PAD., en el Departamento I- Personal del EMGE.

Durante varios años la mencionada sección fue la encargaba de elaborar los diferentes trabajos en lo que se refiere a la administración del personal del Ejército, como también realizar los trabajos requeridos por las diferentes reparticiones del EMGE., asimismo a partir de la gestión 1987 se realizó las impresiones de las diferentes Ordenes Generales del Ejército, (Convocatoria Ascensos, Ascensos y Destinos) trabajos que se continua realizando hasta la fecha.

A partir de la gestión 1989, la sección PAD pasa a formar parte o constituirse como el Centro de Informática Militar del Ejército, asimismo sus dependencias tienen una infraestructura independiente pero sigue dependiendo del Departamento I- EMO, como también continúa realizando los trabajos que requiere la mencionada repartición.

En la gestión 2001 el Centro de Informática Militar del Ejército, deja de ser un Centro y Sección dependiente del Departamento I- EMO. y pasa a formar como una repartición independiente y directamente dependiente de la Jefatura de Estado Mayor General del Ejército, llegando a denominarse como Dirección de Informática Militar del Ejército, desde la indicada fecha se realizaron los trabajos concernientes; Ascensos y Destinos del personal del Ejército, asimismo cubrir los diferentes requerimientos presentados a la DIME. En lo concerniente a listados del personal del Ejército, como también la elaboración de Programas y Sistemas Informáticos para la mejor administración de las reparticiones del EMGE. De acuerdo a sus funciones especificas, trabajos que se realizaron hasta la gestión 2006 primer trimestre.

Finalizando el primer trimestre de la gestión 2006, por disposición de la superioridad, se determinó que el Departamento I- EMO. Se haga cargo de las mencionadas funciones que cumplía la Dirección de Informática Militar, desde esa fecha la DIME, se limito a cumplir con las funciones de Internet,

Mantenimiento de los Equipos de Computación del EMGE., y desarrollar Sistemas Informáticos.

El Avance tecnológico a la época en que se vive y sabiendo que los Ejércitos de todo el orbe usan elementos sofisticados de empleo para la conducción estratégica y táctica para la administración de personal y medios, hizo que el Comando General del Ejercito cree un Centro de Informática Militar con la finalidad de automatizar los procesos de información en todo el ámbito del Ejército, de manera tal que se encuentre a la par de los ejércitos modernos en sus adelantos técnicos.

La Dirección de Informática Militar del Ejercito, fue creado por Orden del Día del Ejercito No. 29/80 de fecha 18 de agosto de 1980, como una Dirección de Apoyo, denominada "CENTRO DE INFORMATICA MILITAR" (CIM).

- Sección de Procesamiento y Automatización de Datos (P.A.D.)
- Centro de Informática Militar del Ejercito (C.I.M.E.)
- Dirección de Informática Militar del Ejercito (D.I.M.E.)

Colombia es un país que no cuenta con los recursos de las naciones consideradas como potencias, no cuenta con programas de vanguardia en desarrollo tecnológico en el área civil o militar; por tal motivo debemos adaptar las tecnologías de otros países a nuestro entorno.

Las tecnologías de la información y las comunicaciones son un conjunto de herramientas, soportes y canales los cuales facilitan el manejo, acceso, procesamiento, almacenamiento, sintetizan, recuperan, registran y permiten difundir contenidos informacionales mediante ordenadores y programas especiales para encontrarla, convertirla, administrarla y transmitirla. Estas han evolucionado desde la invención del telégrafo, el teléfono fijo, la

radiotelefonía, la televisión, el fax, el internet, la telecomunicación móvil y el geoposicionador satelital, lo cual se debe a la revolución tecnológica de la humanidad generalizándose el empleo de redes de comunicación y la globalización de la información.[84]

Actualmente amplían nuestras capacidades de desarrollo físicas y mentales formando parte de la cultura tecnológica que nos rodea y con la que debemos convivir. El avance científico en el marco de la globalización ha transformado nuestras estructuras militares, económicas, sociales y culturales incidiendo en la vida diaria y haciéndolas cada vez mas imprescindibles siendo este su principal aporte ya que nos facilita la realización de nuestro trabajo al permitir obtener información y la comunicación inmediata con los demás.

En las Fuerzas Militares de Colombia ha permitido optimizar los resultados operacionales de nivel estratégico aplicándose también en el ámbito administrativo para planear, dirigir, ejecutar y controlar garantizando el cumplimiento de la misión asignada, lo cual indiscutiblemente se refleja en el significativo desequilibrio de la balanza a nuestro favor colocándola en una posición de no retorno y absoluta desventaja a todos los factores generadores de violencia en nuestro país y especialmente al grupo terrorista de las farc que constituye la amenaza interna.

Estas tecnologías nos han permitido realizar algunas maniobras, pero como las tecnologías son cada vez más asequibles, las tic's están al alcance no solo del gobierno sino también de la delincuencia. Con el uso de de las tecnologías de la información y las telecomunicaciones se interceptan comunicaciones satelitales, telefónicas, radiales, correos electrónicos, se

---

[84]Tecnologías de la información y las telecomunicaciones (Tics), (en línea) Disponible en http://www.monografias.com/trabajos67/tics/tics.shtml

desinforma con la publicación de información errónea en las paginas propias, es el caso de sitios oficiales de la subversión como Anncol (agencia de noticias de la nueva Colombia) que publica información manipulada para su beneficio.

Se accede a bases de datos de computadores, celulares, memorias, discos duros y se conoce la información almacenada en estos, para neutralizar objetivos militares de alto valor estratégico, prevenir acciones terroristas contra la infraestructura del estado, asesinatos y masacres y se recopila material probatorio para la judicialización e individualización de criminales que atentan en contra de la población civil y pretendan realizar asaltos y tomas.

Todos los computadores, discos duros extraíbles y memorias recuperados en operaciones militares conjuntas y de alto valor estratégico como Sodoma o la Fénix por nombrar las más conocidas, facilitaron la realización de importantes capturas de cabecillas de diferentes frentes, se conocieron nexos entre el grupo terrorista de las farc y políticos de nivel regional y nacional, al igual que las relaciones con gobiernos vecinos especialmente con Venezuela y Ecuador. Al momento de salir a la luz pública los diferentes medios registraron en sus publicaciones el "Respaldo militar de las Farc a Chávez, Financiamiento de Chávez a las Farc, Ayuda de Farc a Chávez, Venezuela entrega armas a Farc, Contactos con Ministro del Interior venezolano, Acuerdos con Ministro de Seguridad ecuatoriano, Alianza Farc – Ecuador, Adquisición de Uranio, Pruebas fotográficas"[85], toda esta información recuperada de los computadores que se incautaron en la operación fénix, realizada al campamento de alias Raúl Reyes.

---

[85] Colombia. Revista Semana.com. Las principales revelaciones del computador de 'Raúl Reyes' (en línea) Disponible en http://www.semana.com/on-line/principales-revelaciones-del-computador-raul-reyes/109912-3.aspx, Consultado el 05 de julio de 2011.

"El instituto internacional De Estudios Estratégicos (IISS) analizó durante dos años, con el permiso del gobierno colombiano, los equipos de computación recuperados tras el bombardeo al campamento de Raúl Reyes en marzo de 2008".[86] La Corte Suprema de Justicia determinó que los contenidos de los computadores del jefe de las FARC "Raúl Reyes" no tienen validez dentro de procesos judiciales, porque fueron obtenidas ilegalmente.

"La corte consideró que ese material, que posteriormente fue utilizado en varios procesos contra políticos del país, entre ellos la destituida senadora Piedad Córdoba, fue recolectado por militares que no tenían funciones de policía judicial"[87].

A pesar de la deslegitimación de la información como material probatorio en los juicios de la farc-política, los tres computadores los dos discos duros externos y las tres memorias USB, constituyen una gran cantidad de información que ha posibilitado posteriores planeamientos de operaciones exitosas de alto riesgo y gran importancia.

Operaciones de Alto Riesgo

En general si hablamos de operaciones de alto riesgo, hacemos referencia a absolutamente todas las operaciones en las cuales en su ejecución se pone en riesgo recursos irremplazables y/o están presentes peligros de difícil control. El planeamiento determina los riesgos residuales, los cuales son el nivel de riesgo que continua después de seleccionar controles para los peligros existentes.

---

[86] Colombia. Periódico El Espectador. Com. Los computadores de 'Raúl Reyes' (En línea) Disponible en http://www.elespectador.com/opinion/editorial/articulo-269137-los-computadores-de-raul-reyes, Consultado el 05 de julio de 2011.

[87] Colombia. Actualidad (en línea). http://www.colombia.com/actualidad/noticias/sdi/11158/corte-supremoa-de-justicia-dice-archivos-de-computadores-de-raul-reyes-no-son-pruebas-en-juicios, Consultado el 05 de julio de 2011.

"El instituto internacional De Estudios Estratégicos (IISS) analizó durante dos años, con el permiso del gobierno colombiano, los equipos de computación recuperados tras el bombardeo al campamento de Raúl Reyes en marzo de 2008".[86] La Corte Suprema de Justicia determinó que los contenidos de los computadores del jefe de las FARC "Raúl Reyes" no tienen validez dentro de procesos judiciales, porque fueron obtenidas ilegalmente.

"La corte consideró que ese material, que posteriormente fue utilizado en varios procesos contra políticos del país, entre ellos la destituida senadora Piedad Córdoba, fue recolectado por militares que no tenían funciones de policía judicial"[87].

A pesar de la deslegitimación de la información como material probatorio en los juicios de la farc-política, los tres computadores los dos discos duros externos y las tres memorias USB, constituyen una gran cantidad de información que ha posibilitado posteriores planeamientos de operaciones exitosas de alto riesgo y gran importancia.

Operaciones de Alto Riesgo

En general si hablamos de operaciones de alto riesgo, hacemos referencia a absolutamente todas las operaciones en las cuales en su ejecución se pone en riesgo recursos irremplazables y/o están presentes peligros de difícil control. El planeamiento determina los riesgos residuales, los cuales son el nivel de riesgo que continua después de seleccionar controles para los peligros existentes.

---

[86] Colombia. Periódico El Espectador. Com. Los computadores de 'Raúl Reyes' (En línea) Disponible en http://www.elespectador.com/opinion/editorial/articulo-269137-los-computadores-de-raul-reyes, Consultado el 05 de julio de 2011.

[87] Colombia. Actualidad (en línea). http://www.colombia.com/actualidad/noticias/sdi/11158/corte-supremoa-de-justicia-dice-archivos-de-computadores-de-raul-reyes-no-son-pruebas-en-juicios, Consultado el 05 de julio de 2011.

El fracaso de una operación de alto riesgo pone en evidencia las estrategias adoptadas y pone sobre aviso al enemigo sobre la manera en que se obtuvo información para la planeación de las mismas, desperdicia todos los recursos utilizados, el tiempo y la información que se debió recopilar y analizar para la planeación de la misma, sin mencionar el peligro en el cual se ven inmersos la fuente humana, el personal militar que realiza actividades de infiltración y el personal civil en cautiverio.

Para tomar la decisión o decisiones con base en el riesgo residual, el comandante es quien determina continuar la misión o el curso de acción, si el riesgo es demasiado alto, ordenando controles adicionales, modificar, cambiar o rechazar el curso de acción para el desarrollo o ejecución de la misión.

"Si el riesgo es extremadamente alto la decisión es tomada por el comando superior, si el riesgo es alto la decisión es tomada por el comando superior o por el comandante de la operación".[88]

El uso de la tics se da en las diferentes etapas de cada operación, en la planeación y en la ejecución de las operaciones y su respectiva retroalimentación.

Operación Fénix

Conto con la participación de la Policía, el Ejercito y de la Fuerza Aérea Colombiana. En cercanías de Santa Rosa de Sucumbíos, población ecuatoriana que limita con el departamento colombiano del Putumayo, el 1 de marzo de 2008, fue muerto Luis Edgar Devia Silva, alias 'Raúl Reyes', vocero internacional, miembro del secretariado y segundo cabecilla en la

---

[88] Colombia, Fuerzas Militares de Colombia, Ejercito Nacional, Manual "Organización Estado Mayor y Operaciones", Quinta edición, Publicaciones Ejercito, 2005

estructura de mando de las farc. "Su localización fue posible gracias a un informante y a que Reyes hizo uso de un teléfono satelital."[89]

Operación Jaque

Es una operación especial de inteligencia planeada y ejecutada por inteligencia militar donde se rescatan sanos y salvos 15 de los secuestrados que se encontraban en manos de las FARC. Entre los secuestrados rescatados se encuentran Ingrid Betancourt, los tres ciudadanos norteamericanos y 11 miembros de la Fuerza Pública.

Fueron rescatados en una operación en donde se logró infiltrar la primera cuadrilla de las FARC, comandada por alias Cesar. A través de suplantaciones en las comunicaciones por radio entre los frentes y diferentes procedimientos logrando también infiltrar al secretariado. Como los secuestrados estaban divididos en tres grupos, se consiguió que se reunieran en un solo sitio y luego se facilitara su traslado al sur del país para que supuestamente pasaran directamente a órdenes de Alfonso Cano.

"El Plan Colombia permitió la transferencia de tecnología de punta y experiencia, con particular énfasis, en las áreas de inteligencia y operaciones especiales que fueron fundamentales en el logro de los altos niveles de capacidad profesional que hoy tienen nuestras Fuerzas Armadas".[90]

---

[89] Colombia, Comando General de las Fuerzas Armadas de Colombia, Operación Fénix, http://www.cgfm.mil.co/CGFMPortal/Operaciones/Reyes/prontuario/prontuario_reyes.swf. Consultado el 07 de julio de 2011.

[90] Colombia, Comando General de las Fuerzas Armadas de Colombia, Operación Jaque, Jaque... ¡Operación perfecta!, General FREDDY PADILLA DE LEÓN http://www.cgfm.mil.co/CGFMPortal/Operaciones/jaque_web/OperacionJAQUE/Articulo_Gen Padilla_OpeJaque.pdf. Consultado el 07 de julio de 2011

"Igualmente, el apoyo brindado por el Gobierno de Estados Unidos y sus Fuerzas Armadas para esta operación, en los aspectos relacionados con inteligencia de imágenes y capacidad de comunicaciones de última generación".[91]

Se instalaron en los helicópteros tres dispositivos de alerta que se emplearían en caso necesario, emitirían una señal de alerta en caso de que se presentara algún imprevisto que pusiera en peligro la misión, de igual manera se instalo en los cascos de los pilotos dispositivos de comunicación satelital que mantenían intercomunicados a todos los integrantes de la operación con el puesto de mando ubicado en Bogotá; Un avión a 30000 pies de altura servía como repetidor de las comunicaciones en tiempo real .

"Para la conducción y mando de la Operación Jaque, en sus dos fases, se requirió del apoyo de tecnología de punta en comunicaciones, la cual permitió el seguimiento minuto a minuto de toda la operación desde la Sala de Comando y Control en el Cuartel General de las Fuerzas Militares en Bogotá"[92] con el sistema integrado de comando y control.

Tres operaciones tuvieron incidencia en el éxito de la Operación Jaque: la Operación Tifón, el 28 de abril de 2007, que permitió consumar el escape y la libertad del subintendente John Frank Pinchao; la Operación Fénix, el 1 de marzo de 2008, en la cual se causó la muerte en combate al segundo hombre de las Farc; y la Operación Elipse, en febrero de 2008, que facilitó observar a los ciudadanos estadounidenses en poder de las Farc, cuando ellos se bañaban en el río Apaporis (en el suroriente colombiano).

---

[91] Colombia, Comando General de las Fuerzas Armadas de Colombia, Operación Jaque, Op.Cit.

[92] Ibíd.

"Es de anotar que para la ejecución de la Operación Jaque fueron procesadas informaciones suministradas por desmovilizados y por el subintendente Pinchao".[93]

Operación Sodoma

"Los organismos de seguridad que adelantaron el operativo interceptaron una comunicación de la guerrilla en la que se pedía unos zapatos especiales, los cuales fueron enviados con un localizador GPS que permitió establecer la plena ubicación del "Mono Jojoy" en La Serra de la Macarena (Meta), donde fue muerto en combate".[94]

Según reveló RCN La Radio, gracias a un localizador electrónico camuflado en un calzado especial que necesitaba utilizar el guerrillero, fue que la Fuerza Pública logró ubicar y neutralizar el objetivo estratégico militar y nacional. "También se recuperaron 60 memorias USB y 20 computadores"[95] con valiosa información que seguramente, será el punto de partida para nuevas operaciones exitosas que nos acerquen al fin del conflicto interno.

Toda la flota de aeronaves de la fuerza aérea Colombiana cuenta con el sistema integrado de comando y control, que le permite la comunicación, control y monitoreo con el CECOFA (centro de comunicaciones de la fuerza aérea) desde el momento en que se encienden los motores, brindando datos

---

[93] Colombia, Comando General de las Fuerzas Armadas de Colombia, Operación Jaque, Op. Cit.

[94] Colombia, Así fue la operación 'Sodoma' que dio muerte a 'Jojoy' http://www.semana.com/nacion/operacion-sodoma-dio-muerte-jojoy/144996-3.aspx Consultado el 07 de julio de 2011

[95] Colombia, Así se planeó y ejecutó la Operación 'Sodoma' http://www.eltiempo.com/archivo/documento/CMS-7960880, JINETH BEDOYA LIMA ENVIADA ESPECIAL DE EL TIEMPO* LA MACARENA (META) * Con la Redacción Justicia en Bogotá. Consultado el 07 de julio de 2011

de velocidad, altura y coordenadas en tiempo real, gracias al uso integrado del geo posicionado satelital. "Este tipo de tecnología se conoce la ubicación exacta de las aeronaves en el espacio aéreo y en tierra, lo que ha prevenido colisiones y accidentes y ha facilitado la recuperación de los restos en caso de sufrir una falla o ataque".[96]

En las Fuerzas Militares de Colombia ha permitido optimizar los resultados operacionales de nivel estratégico aplicándose también en el ámbito administrativo para planear, dirigir, ejecutar y controlar garantizando el cumplimiento de la misión asignada, lo cual indiscutiblemente se refleja en el significativo desequilibrio de la balanza a nuestro favor colocándola en una posición de no retorno y absoluta desventaja a todos los factores generadores de violencia en nuestro país y especialmente al grupo terrorista de las farc que constituye la amenaza interna.

[96] Información obtenida de piloto oficial de aviación de Ejército que participo en la operación Jaque, obtenido de manera personal el 13 de julio de 2011.

CONCLUSIONES

Debido al enfrentamiento de retos, en el siglo pasado no se podía, ni imaginar, en un mundo donde todo es sometido al juicio de la opinión pública a través de los medios de comunicación. Ahora bien, las Fuerzas Militares, brindan herramientas para fortalecer la inteligencia y de esta forma manejar dispositivos a distancia que permitan mantener la integridad de la fuerza en misiones de alto riesgo puesto que requieren adentrarse en territorios dominados por fuerzas enemigas sin que éstas perciban la presencia y el desarrollo de tareas que facilitan el planeamiento estratégico nacional y militar.

Durante las operaciones militares la presión mediática se incrementa hasta tal punto que constituye un factor más en el planeamiento y ejecución de las operaciones. De su correcta ejecución depende en buena medida la valoración que haga la sociedad y a su vez influirá sobre la toma de decisiones de gran repercusión sobre la operación.

Las nuevas tecnologías han revolucionado el mundo de la información, su evolución es más rápida que la capacidad de adaptación de los ejércitos regulares. La velocidad a la que se trasmite una información supera la capacidad de respuesta con los procedimientos convencionales y ello solo se puede resolver con agilidad de respuesta. Salvo que exista una unidad de criterio. ¿La clave? Instrucción y planeamiento, esenciales para un correcto y adecuado uso de la información.

Ahora bien, el avance tecnológico, ha causado una revolución en la forma de pensar, de vivir, y hasta de vincularse, tanto del hombre con su par, como del hombre con las cosas. Internet, es el ejemplo claro de uso y abuso de dicha herramienta para toda clase de fines.

Las técnicas informáticas y la comunicación en las operaciones Militares, en un mundo globalizado como se vive ha sido el resultado de los cambios permanentes que ha sufrido el entorno mundial y de las necesidades que siempre están presentes en el hombre, como también el incesante cambio de las tecnologías y avances en comunicación permiten sin duda obtener estos medios para así lograr el éxito en las operaciones militares.

BIBLIOGRAFIA

- Agencia de Información Internacional de Rusia "RIA Novosti". .http://sp.rian.ru/high_tech/20110715/149739230.html
- Agencia Latinoamericana de Información. Facebook y Twitter: trincheras de la netwar http://alainet.org/active/36476&lang=es
- APPLEGALE MELISA, Informe publicado sobre Ciencia y Tecnología publicado por El Stralegre Studies Institute
- ARMSTRONG, Richard N. Red Army Tank Commanders: The Armored Guards. Atglen, Penn.: Schiffer Military History, 1994.
- Arquilla, John. Y Ronfeldt, David. Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político. http://dialnet.unirioja.es/servlet/libro?codigo=232687.
- Arquilla, J. y Ronfeldt, D. (1996), El advenimiento de la guerra red, California, RAND Corporation, p. 49. Publicado por la Universidad Javeriana - Colombia. Forigua Rojas, Emersson. (2006) LAS NUEVAS GUERRAS: UN ENFOQUE DESDE LAS ESTRUCTURAS ORGANIZACIONALES.http://www.javeriana.edu.co/politicas/publicaciones/documents/9LASNUEVAS.pdf.
- Artículos destacados. Nato se prepara para una ciberguerra. http://www.neoteo.com/nato-se-prepara-para-una-ciberguerra-15578.
- Articulo Nazi, en: Friedrich Kluge, Elmar Seebold:Etymologisches Wörterbuch der deutschen Sprache, Walter de Gruyter Auflage, Berlin/New York 2002
- CALCAGNO Eduardo, Propaganda, la comunicación política en el siglo XX, Comunicación Gráfica Edición y Diseño, 1992.
- Asociación Internacional de Comunicaciones y Electrónica de las Fuerzas Armadas (AFCEA Internacional). AFCEA Argentina http://www.afcea.org.ar/cursos/OpInfo.htm.
- BARRIOS EDGARDO Martin, Profesor Universitario en Informática aplicada – Facultad de Ingeniería, Universidad Nacional del Chaco – Argentina. www.answers.yahoo.com/question/index

- CANO, J. (2008) La guerra fría electrónica y la inseguridad de la información. Publicación en Blog.http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=450012245&random=4197

- Colombia. Revista Semana.com. Las principales revelaciones del computador de 'Raúl Reyes' http://www.semana.com/on-line/principales-revelaciones-del-computador-raul-reyes/109912-3.aspx,

- Colombia. Periódico El Espectador. Com. Los computadores de 'Raúl Reyes'. http://www.elespectador.com/opinion/editorial/articulo-269137-los-computadores-de-raul-reyes.

- Colombia. Actualidad. http://www.colombia.com/actualidad/noticias/sdi/11158/corte-supremoa-de-justicia-dice-archivos-de-computadores-de-raul-reyes-no-son-pruebas-en-juicios,

- Colombia, Fuerzas Militares de Colombia, Ejercito Nacional, Manual "Organización Estado Mayor y Operaciones", pagina Quinta edición, Publicaciones Ejercito, 2005

- Colombia, Comando General de las Fuerzas Armadas de Colombia, Operación Fénix, http://www.cgfm.mil.co/CGFMPortal/Operaciones/Reyes/prontuario/prontuario_reyes.swf.

- Colombia, Comando General de las Fuerzas Armadas de Colombia, Operación Jaque, Jaque... ¡Operación perfecta!, General FREDDY PADILLA DE LEÓN

http://www.cgfm.mil.co/CGFMPortal/Operaciones/jaque_web/OperacionJAQUE/Articulo_GenPadilla_OpeJaque.pdf.

- Colombia, Así fue la operación 'Sodoma' que dio muerte a 'Jojoy' http://www.semana.com/nacion/operacion-sodoma-dio-muerte-jojoy/144996-3.aspx.

- Colombia, Así se planeó y ejecutó la Operación 'Sodoma' http://www.eltiempo.com/archivo/documento/CMS-7960880, JINETH BEDOYA LIMA ENVIADA ESPECIAL DE EL TIEMPO* LA MACARENA (META) * Con la Redacción Justicia en Bogotá.

- Cuba. Cuba debate. Círculo de Periodistas Cubanos contra el Terrorismo. En Video y Fotos exclusivas: El agente Raúl revela operación de la CIA. http://www.cubadebate.cu/noticias/2011/03/08/en-video-y-fotos-exclusivas-el-agente-raul-revela-operacion-de-la-cia/.

- China, preparándose para una ciberguerra. http://www.pcworld.com.mx/Articulos/6408.htm.

- Ciberguerra – Red seguridad. http://www.borrmart.es/articulo_redseguridad.php?id=458&numero=17 José Ramón Borredá.

- Ciberguerra en dos actos. http://alt1040.com/2011/01/.

- Ciberguerra, stuxnet y gente con tejado de vidrio. http://publicogt.com/2011/06/14/ciberguerra-stuxnet-y-gente-con-tejado-de-vidrio/

- Declaraciones de Barry Collin: http://www.af.mil/news/Feb1998/n19980206_980156.html

- Deisy Francis Mexidor. digital@juventudrebelde.cu. http://www.juventudrebelde.cu/cuba/2011-03-21/ciberguerra-mercenarismo-en-la-red/

- Deisy Francis Mexidor.. http://www.juventudrebelde.cu/cuba/2011-03-21/ciberguerra-mercenarismo-en-la-red/ digital@juventudrebelde.cu.

- Del El Diario Digital: Edición Cd. Juárez. Toman Adicción por Web. 18 de Noviembre 2005.

- Documento informativo del ieee 09/2011, Nuevo concepto de Ciberdefensa de la OTAN (marzo de 2011).
- Documentación seguridad. Documentación relacionada con la gerencia de riesgos y los seguros.www.mapfre.com/gerencia-riesgos. http://www.neoteo.com/nato-se-prepara-para-una-ciberguerra-15578.
- Ejército de Chile, artículo "la logística y la Guerra del golfo Pérsico y la Guerra en Irak (2003), año 2006.
- Embajada de los Estados Unidos en Bogotá. Apartes del Discurso de la Secretaria de Estado Hillary Clinton sobre Libertad en Internet.http://spanish.bogota.usembassy.gov/pr_018_15022011.html.
- Entrevista televisiva realizada en Suecia para el programa televisivo Rapport, noviembre 3, 1994. El audio de la entrevista completa (en inglés) se puede escuchar en: http://www.josefsson.net/gibson/
- Estados Unidos, Extracto del testimonio prestado por Dorothy E. Denning ante el Special Oversight Panel on Terrorism, Committee on Armed Services, de la cámara baja estadounidense, 23 de mayo de 2000. Ver texto completo en http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
- Francia. Presseurop.eu. Ciberdefensa Estonia forma un ciber ejército http://www.presseurop.eu/es/content/news-brief-cover/462031-estonia-forma-un-ciber-ejercito-modification.
- G charon, J-M., Mercier, a. (coord.). (2004). Armes de communication massive. Information's de guerre en Irak: 1991-2003. Paris: cnrs Editions.
- García Fajardo, J.C. (1992-05-26): Comunicación de masas y pensamiento político http://www.educacionplasticavisual.es/?cat=5

- Germán Leyens. Rebelión. http://english.aljazeera.net/indepth/opinion/2011/06/20116673330569900.html.
- GLANTZ, David M. Soviet Military Operational Art: In Pursuit of Deep Battle. London; Portland, Or.: Frank Cass
- Guerrillero. Ciberguerra y terrorismo. http://www.guerrillero.cu/index.php?option=com_content&view=article&id=7525:ciberguerra-y-terrorismo-mediatico-nueva-modalidad-de-agresion&catid=37:opinion&Itemid=57.
- Identidad Nacional y Natural. http://identidadlra9.blogspot.com/2011/06/el-pentagono-concluye-que-los.html.
- Impre.com. Militares de EEUU. http://www.impre.com/noticias/nacionales/2011/6/22/militares-de-eeuu--entrenados--261454-1.html#commentsBlock.
- Información obtenida de piloto oficial de aviación de Ejército que participo en la operación Jaque, obtenido de manera personal en 13 de julio de 2011.
- INTERFICTO, ¿Qué es el Ciberespacio? Puede consultarse en el sitio www.articulo.org/articulo/25407/que_es_el_ciberespacio.html
- ITU (2010) Global cybersecurity agenda. http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf.
- Jordán, Javier y Torres, R. Manuel. "Internet y actividades terroristas: el caso del 11-M", El profesional de la información, v. 16, n. 2, marzo-abril de 2007, págs. 123-130
- JOSROJAVAR FARTHARD. Los nuevos Mártires de Ala. Ediciones MR, 2003
- Kershaw, Ian. (1999) Hitler ISBN 0-393-04671-0 Berlin.

- La guerra que viene..http://www.neoteo.com/ciberguerra-la-guerra-que-viene.
- La ciberguerra pasa al ataque.html. http://blasapisguncuevas.blogcindario.com/2010/06/05803-
- La ciberguerra se considera una amenaza real. La Nación. http://www.lanacion.com.ar/1228365-la-ciberguerra-ya-es-considerada-una-amenaza-real
- La nación.com. Ciberguerras sin balas ni sangre. http://www.lanacion.com.ar/1213586-ciberguerras-sin-balas-ni-sangre
- Maestros del Web. Georgia, la nueva víctima del ejército cibernético Ruso. http://www.maestrosdelweb.com/actualidad/georgia-la-nueva-victima-del-ejercito-cibernetico-ruso/.
- Madrid, España. El país.com. Los troyanos espían en Alemania, China y los servicios secretos de Berlín, en el ojo del huracán por los ataques electrónicos. http://www.elpais.com/articulo/reportajes/troyanos/espian/Alemania/elpepusocdmg/20070902elpdmgrep_5/Tes.
- Manuel Castells. http://www.lavanguardia.com/opinion/articulos/20101211/54086305259/la-ciberguerra-de-wikileaks.html.
- MATAMALA APARICIO Salvador, Guerra de la Informática, monografías Chile 13 de enero de 2009. http://www.ufro.cl/corporativa/docs/Memoria%20Institucional, 20 UFRO/202/06.
- MORA PARDO Álvaro, Globalización, Interdependencia compleja y disuasión.
- Nato se prepara para una ciberguerra. http://www.portalnet.cl/comunidad/archive/index.php/t-187334.html.
- Neoteo. Ciberguerra. http://www.neoteo.com/ciberguerra-la-guerra-que-viene.
- Oscar Pin – Consultor TIC. http://oscarpin.com/2010/12/07/wikileaks-la-primera-ciberguerra-de-la-historia/

- Página web del Ejército de Chile, www.ejercito.cl, comunicados de prensa por ayudas a la población.

- Pisani, Francis. Le Mondé Diplomatique (El mundo Diplomático) Edición Cono Sur. Nueva guerra contra nuevo enemigo. Número 36 - Junio 2002, páginas 10-11

- Publicaciones de la RED en.medi@:en.re.dando: http://www.enredando.com

- Publicado en, nuevo orden mundial, atentados, noticia, tecnología, monitoreo y vigilancia, censura y opresión por Gonzalo Fernández en octubre 14 2010

- Reig, Ramón (1995): El control de los medios de comunicación de masas: bases estructurales y psicosociales http://www.laislalibros.com/libros/control-de-la-comunicacion-de-masas

- SALELLAS Luciano, Delito informático y ciberterrorismo pueden consultarse en el sitio http://www.forodeseguridad.com/artic/discipl/4075.htm

- Strategy page. http://www.strategypage.com. http://poderiomilitar-jesus.blogspot.com/2011/07/corea-del-sur-crea-la-guerra.html.

- Terrorismo.com. Las definiciones del FBI y el Departamento de Estado pueden consultarse en http:// www.terrorismo.com.

- Thomas, Timothy L. Las estrategias electrónicas de China". Military Review, Julio-Agosto de 2001, pág. 72ss.

- TREJO DELBARNE, Raúl: La nueva alfombra mágica. Usos y mitos de Internet, la red de redes. http://www.nua.ie/surveys/how_many_online/index.html

- Universidad Nacional Autónoma de México. Subdirección de Seguridad de la Información (SSI). Ataques cibernéticos georgianos sólo civiles, dice informe. http://www.seguridad.unam.mx/noticias/?noti=3319.

"TOMAS RUEDA VARGAS"
054882