El dominio del ciberespacio y de las tecnologias de información y comunicaciones, como un nuevo poder del campo militar

Franklin Herrera Suarez

Trabajo de grado para optar al título profesional:

Maestría en Seguridad y Defensa Nacionales

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

2009

MONOGRAFÍA DE GRADO

"EL DOMINIO DEL CIBERESPACIO Y DE LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES, COMO UN NUEVO PODER DEL CAMPO MILITAR"

FRANKLIN HERRERA SUAREZ

MAESTRÍA EN SEGURIDAD Y DEFENSA NACIONALES

ESCUELA SUPERIOR DE GUERRA DE COLOMBIA

BOGOTÁ D.C., JULIO 2009

ÍNDICE

INTRODUCCIÓN

Hace unos años se decía que la nación que tenga la información tendría el poder. Pero este concepto ha evolucionado, para decir que la nación que tenga la información y la capacidad para usarla en su favor tendrá el poder.

Las naciones han comenzado a valorar la información digital como uno de los activos más valiosos, y ha depender cada vez más de los sistemas de información que la administran.

Colombia como un país en desarrollo y partícipe del proceso de globalización, no se ha aislado del fenómeno de las redes interconectadas de datos como Internet. Por lo cuál, es pertinente estar preparados para enfrentar las nuevas amenazas de carácter global y asimétrico provenientes del ciberespacio.

El Ciberespacio se puede ver como un nuevo campo de batalla, en el cuál se pueden aplicar los mismos principios de la guerra y sus estrategias.

La política de defensa de Colombia como estado actualmente esta centrada en el conflicto interno y el narcotráfico. Pero al comenzar a hablar de postconflicto. Se puede considerar un momento oportuno para preparar la nación, para contrarrestar las nuevas amenazas terroristas que a nivel mundial. Que pueden atentar contra el estilo de vida de la sociedad en la era de la información.

El propósito de esta monografía, es el de justificar y analizar el empleo con carácter militar del Ciberespacio, y las tecnologías de información y comunicaciones (TIC). Igualmente generar recomendaciones para el estado colombiano. Orientadas a aprovechar y mejorar el uso del Ciberespacio y las TIC, en el actual conflicto interno y a futuro prepararse para las posibles nuevas amenazas asociadas al uso de las anteriores tecnologías.

La monografía comenzará su análisis a partir de la Guerra del Golfo en 1991, por ser considerado un momento histórico. En el cual se emplearon las tecnologías de información y comunicaciones, por parte de la fuerzas de la coalición para ayudar a vencer a sus adversarios. Los análisis siguientes estarán enmarcados en el empleo actual, de las nuevas tecnologías de comunicaciones en el ámbito del Ciberespacio e Internet desde el punto de vista militar.

El primer capítulo, "El surgimiento de las tecnologías de información y comunicaciones, como una nueva arma a partir de la Guerra del Golfo". Analiza como la tecnología de información y de comunicaciones empleada durante la Guerra del Golfo en 1991, impactó en la forma como se desarrollarían futuros conflictos.

Revisa el empleo de las bombas inteligentes, los centros de comando, control y comunicaciones y las operaciones de información. Ilustra como estas tecnologías actualmente se emplean en el conflicto interno colombiano. Como lo son las bombas inteligentes en operaciones exitosas en contra de los cabecillas de las FARC, operaciones de información en Internet como la Operación Jaque.

Concluye como a partir de este conflicto, se vislumbra la aparición en escena de un cuarto poder militar, consistente en el dominio de las nuevas tecnologías de información y comunicaciones. La Guerra del Golfo presentó al mundo el poder de las redes de comunicaciones, y sería el preámbulo de como hoy día se emplea Internet en la guerra.

El segundo capítulo, "Comando, control y comunicaciones: una herramienta clave en la estrategia militar". Analiza como los centros de comando, control y comunicaciones han evolucionado hasta los modelos de centros interconectados gracias a redes de comunicaciones globales.

Revisa como las tecnologías de información han impactado en la velocidad de cómo se toman decisiones en el campo militar. Desde los tiempos del envío de un documento en

ferrocarril, hasta hoy día, con solo oprimir una tecla del computador, en cuestión de segundos se recibe la información gracias al correo electrónico.

Capacidades enlazadas a los sistemas de vigilancia remotos como los satélites, los equipos de transmisión de video en tiempo real, brindan a los comandantes el poder de tener una mejor visión del campo de batalla y así poder mejorar su estrategia.

Paralelo a estos cambios, las organizaciones militares se han adaptado para optimizar el uso de los recursos en las guerras y mejorar su efectividad. Tal es el caso de los comandos conjuntos de operaciones, como los empleados durante la Guerra del Golfo para garantizar el control de las operaciones de los miembros de la coalición. Y en Colombia el caso del Comando Conjunto No.1 del Caribe, que agrupa las fuerzas armadas de la zona norte del país.

Finalmente se presentan las ventajas de implementar en Colombia un nuevo modelo de comando, control y comunicaciones, basado en un modelo de red colaborativa que permitirá potenciar la información y el conocimiento adquirido en el actual conflicto interno, y en caso de agresiones externas.

El tercero capítulo, "La necesidad de diseñar para Colombia una estrategia de seguridad nacional, para la protección del ciberespacio". Analiza el porque Colombia como una nación que no se ha aislado del proceso de globalización, ni del proceso incorporación de las nuevas tecnologías de información y de comunicaciones en el sector privado, público y de defensa. Debe preparar prontamente una estrategia nacional para la protección del ciberespacio.

Analiza el caso de Estonia / Rusia, por ser considerada la primera guerra electrónica del siglo XXI. Guerra que se libró a través de la red global de datos Internet, a diferencia de sus predecesoras como la del Golfo que se libró sobre el espectro electromagnético.

Revisa el porqué a nivel estratégico el ciberespacio es el campo ideal de batalla, sobre el cuál emplear estrategias de poder invisible o "soft power". Para el caso colombiano se recomienda implementar estrategias defensivas, ante la evidencia que las guerras electrónicas hacen parte de los nuevos conflictos que se están presentando.

El cuarto capítulo, "El ciberespacio como nuevo escenario geopolítico: Retos y recomendaciones para Colombia". Se explica el porque adicional a los tradicionales espacios de tierra, mar, aire y espacio exterior, el Ciberespacio debe considerarse como un nuevo espacio a tener en cuenta por parte de la geopolítica y como aprovecharlo.

Presenta casos de uso del Ciberespacio para su análisis geopolítico. El caso de Al Qaeda y la Yihad Islámica. El caso del 4 de Febrero de 2008 en Colombia, cuando gracias a las redes sociales de Internet. Se logró gran movilización mundial contra las FARC. El caso del monitoreo del espectro electromagnético por parte de Estados Unidos, a través del proyecto Echelon y Carnivore.

Ilustra algunos de los retos que gracias a la penetración masiva de las telecomunicaciones en Colombia, se presentan como la inseguridad informática, las nuevas leyes de protección de datos, los procesos de investigación y desarrollo.

Concluye el cuarto capítulo recomendando la necesidad apremiante para Colombia de establecer estrategias para aprovechar el Ciberespacio y el poder blando que brinda la información. Igualmente crear políticas y estrategias de defensa ante posibles amenazas internas o externas en el Ciberespacio de Colombia.

Finalmente el quinto capítulo, "Necesidad de una política de Ciberdefensa en Colombia". Plantea la necesidad de establecer una política de defensa del ciberespacio de Colombia por parte del gobierno nacional.

Revisa las políticas de ciberdefensa de algunas naciones líderes en la era de la información. Y presenta las acciones tomadas por el gobierno colombiano con respecto a la ciberseguridad. Con el propósito, de dar argumentos para crear políticas de carácter preventivo ante las nuevas amenazas provenientes del Ciberespacio.

Finalmente, presenta recomendaciones sobre algunas de las posibles acciones a seguir, para fortalecer los niveles de la Ciberdefensa de la nación.

CAPÍTULO I

EL SURGIMIENTO DE LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES, COMO UNA NUEVA ARMA A PARTIR DE LA GUERRA DEL GOLFO.

INTRODUCCIÓN

Al revisar el avance de las nuevas tecnologías militares como lo son los misiles guiados por láser, los centros de comando, control y comunicaciones integrados y los sistemas de vigilancia satelital, entre otros usados en la guerra del Golfo. Se puede afirmar que su utilización exitosa, cambió la forma como las guerras se pudieran desarrollar en el futuro.

Este capítulo pretende mostrar como las tecnologías de información y comunicaciones (TIC) empleadas en 1991, marcaron un hito en la historia de las revoluciones en asuntos militares dando la bienvenida al empleo del poder de la información en los posteriores conflictos.

Es así como la tecnología al ser usada con ingenio por el hombre, se torna en un elemento capaz de cambiar el curso de acción de un conflicto. Según Clausewitz las fricciones entre los seres humanos y los gobiernos siempre estarán presentes, esto hace parte de la naturaleza intrínseca de cada ser. Pero lo que si puede variar es la forma de hacer la guerra, los medios empleados y los fines. Es en los medios y fines donde la tecnología combinada con el ingenio del estratega ayuda a cambiar el resultado de las guerras.

Los estrategas deben entender primero al enemigo, su forma de lucha, efectuar la respectiva valoración de potenciales, visualizar los posibles escenarios de la guerra y en ese momento si emplear la tecnología militar de la forma más eficiente y efectiva posible.

El estratega no debe pensar en función de la tecnología militar, debe planear su estrategia a partir de los fundamentos lógicos estratégicos y luego de tenerla planteada. Hacer uso de las tecnologías que se requieran, para cumplir con los objetivos trazados.

Durante la guerra del Golfo, no solo se combatió en el campo en los terrenos desérticos, o en medio de los campos petrolíferos. Gracias a las nuevas tecnologías se pudo llevar el combate al campo de los medios de comunicación y a los aspectos sicológicos basados en operaciones de información.

1. EMPLEO DE LAS NUEVAS TECNOLOGIAS EN LA GUERRA DEL GOLFO

El empleo de nuevas tecnologías militares y su uso innovador han estado presentes en el desarrollo de las guerras libradas a través de la historia de la humanidad. Es así, como la tecnología actuó como un medio facilitador para ganar la guerra del golfo por parte de la coalición conformada por 34 países. Liderada por Estados Unidos bajo el mando de las Naciones Unidas.

Durante la ejecución de este conflicto se probaron varias innovaciones como la tecnología para evitar los radares, las bombas inteligentes guiadas por láser, los centros de comando y control conjuntos para coordinar las operaciones aéreas entre países de la coalición, todos los vehículos dotados con sistemas de identificación amigo o enemigo, cada aeronave con transmisión de video abordo, las nuevas técnicas de propaganda dentro del marco de las guerras de información empleadas en operaciones sicológicas.

Antes de revisar cada una de las tecnologías que mas aportaron a la victoria, es conveniente citar los objetivos planteados por el presidente Bush para limitar el conflicto: retiro incondicional y completo de todas las fuerzas iraquíes de Kuwait, la reinstauración del

gobierno legítimo de Kuwait, la seguridad y estabilidad del Golfo Pérsico y la protección de los ciudadanos estadounidenses en el extranjero[1].

Basados en los anteriores planteamientos, los Estados Unidos limitaron sus fines a retomar el territorio de Kuwait con le mínimo de perdidas humanas posibles y en un muy corto período de tiempo. Para lo cuál plantearon la estrategia a emplear, basada en una primera fase de ataques aéreos de alta precisión y afectación del enemigo.

Atacando primero los centros de comando, control y comunicaciones, con el propósito de generar un efecto de "niebla de la guerra" en sus tropas. En una segunda fase emplear las tropas en tierra para una retoma del territorio y su consolidación, en coordinación conjunta con la armada y fuerza aérea.

Se puede observar que uno de los objetivos de la guerra, no era para ese momento derrocar a Sadam Hussein. Ya que mantener a Saddam en el poder le daba a Estados unidos, Israel, Arabia Saudita y Kuwait un enemigo común para seguir aplicando una estrategia de compromiso con los países amigos de la región.

Al plantear su estrategia de guerra los Estados Unidos, se presentó un gran reto. Desvirtuar el efecto de confiar excesivamente en la tecnología, generado durante la guerra de Vietnam. Ya que en Vietnam la guerra de guerrillas y la geografía, no permitieron que fuera empleada exitosamente. Pero en la guerra del golfo las condiciones cambiaron, y la valoración de potenciales fue llevada a cabo correctamente.

Lograr el éxito de esta acción militar era clave para los Estados Unidos, con el fin de apalancar su economía. Ya que posterior a la Guerra Fría, se debía ratificar su papel como la superpotencia a nivel mundial. La economía americana posterior a la Guerra del Golfo logró llegar a uno de sus mejores puntos, debido en parte al nivel del gasto militar invertido y las tecnologías desarrolladas.

---

[1] BUSH, George. *The Deployment of US Armed Forces to Saudi Arabia*, discurso del 8 de agosto de 1990.

2. EMPLEO DE LAS BOMBAS INTELIGENTES

En la guerra del golfo se ratificó de nuevo la tesis expresada por Giulio Douhet de la utilización del poder aéreo en las operaciones militares. Su tesis de la construcción de nuevos aviones que permitieran ejecutar la teoría de bombardeo profundo, se vio empleada gracias al diseño de los aviones con tecnología antirradar encargados de los bombardeos dentro de territorio iraquí.

El concepto de bombardeo profundo, consiste en bombardear activos estratégicos del enemigo, que se encuentren ubicados en las ciudades donde se concentre la población. Esto con el objetivo, de minar la moral de la población y llevar la guerra al interior de la nación enemiga[2].

La campaña aérea que duró las seis primeras semanas se orientó por parte de los aliados para que se desarrollara de manera asimétrica, ya que desde el principio los bombardeos destruyeron la fuerza aérea iraquí en tierra, igualmente esta no recibió ayuda de otros países para enfrentarse a las aeronaves de combate de los aliados.

Durante este conflicto se probó el uso de la nueva tecnología de "bombas inteligentes". Las cuáles se probaron inicialmente durante la guerra de Vietnam. Uno de los aviones bombarderos lanzaba la bomba, y el otro avión dirigía el rayo láser sobre el objetivo para que el misil diera en el blanco.

En la operación "Tormenta del Desierto", como se denominó a la campaña liderada por Estados Unidos para liberar Kuwait. Debutaron los misiles que trasmitían en tiempo real la

---

[2] SHINER, John F. *Reflections on Douhet the classic approach.* Air University Review, 1986. http://www.airpower.au.af.mil/airchronicles/aureview/1986/jan-feb/shiner.html. última consulta julio 15 de 2009.

señal de video antes de impactar sobre su objetivo. Se lanzaron 244 bombas guiadas por láser y 88 misiles crucero que impactaron en Irak, de un total de 250,000 bombas arrojadas durante la guerra[3].

Es de anotar que no todos los bombardeos se realizaron apoyados en bombas inteligentes. Solo el 2% de los ataques las usaron, pero impactaron el 40% de los blancos de gran importancia estratégica. Los blancos de estos ataques se establecían a partir de la información entregada por fuentes de inteligencia humana y técnica.

Gracias a la efectividad y ubicación de los bombardeos, empleando bombas inteligentes. La moral del pueblo iraquí y de su ejército se vio disminuida, lo cuál sería posteriormente aprovechado por las operaciones de información que se lanzaron sobre las tropas invasoras en Kuwait.

Debido al síndrome del fracaso en Vietnam, esta campaña se concibió desde un principio para minimizar el número de pérdidas humanas de los integrantes de la coalición.

Estados Unidos identificó las vulnerabilidades del enemigo, y diseño ataques aéreos empleando tecnología de alta precisión durante los bombardeos, empleó tácticas de guerra sicológica y de información para ir minando la voluntad de lucha de los combatientes iraquíes, operó desde un principio de manera conjunta la fuerza aérea, armada y ejercito para luego garantizar el éxito en la campaña terrestre.

A partir del conflicto de la Guerra del Golfo y de su transmisión en vivo gracias a CNN, las bombas inteligentes ayudaron a crear una idea de la guerra no sangrienta. Las bombas guiadas por GPS son tan precisas como la inteligencia lo es. Se emplearon exitosamente en

---

[3] *Gulf War strikes marked a sea change in air tactics.* http://www.cnn.com/SPECIALS/2001/gulf.war/legacy/airstrikes/index.html. Última consulta Noviembre 22 de 2008

la campaña de Kosovo en 1999, cerca de 22000 bombas las cuáles impactaron exitosamente el 50% de lo blancos[4].

Aunque, el ataque a la embajada china en Belgrado (Yugoslavia) por parte de la OTAN, fue uno ejemplo de los posibles errores que la inteligencia humana puede causar al despersonalizarse el conflicto[5]. Posteriormente en la operación de liberación de Afganistán, se logró alcanzar un 75% de precisión en las bombas[6].

En el caso de Colombia, se han empleado en la lucha contra las FARC armamento inteligente. Gracias al uso de esta clase de armas, se han podido neutralizar importantes cabecillas como el 'Negro Acasio' y 'Raúl Reyes'[7].

La ciberguerra también se emplea actualmente en el conflicto colombiano. El uso de aviones de inteligencia no tripulados que envían sus transmisiones de video en tiempo real, ha facilitado la toma de decisiones en corto tiempo. Tecnologías de información, que permiten en tiempo real captar comunicaciones de la guerrilla, monitorear conversaciones telefónicas y correos electrónicos vía Internet. Este uso de la tecnología de comunicaciones en esta clase de conflicto asimétrico, ha obligado a que las FARC retornen al empleo de correos humanos.

En la era de la información las armas inteligentes ayudan en parte a ganar la guerra, pero es el comandante que tenga la mejor información del campo de batalla y la mejor habilidad para la toma de decisiones quien puede ganar las batallas. Esto equivale, a disminuir la

---

[4] BERKOWITZ, Bruce. *The new face of war, How war will be fought in the 21st Century*. New York, Ed. Free Press. 2003. Pág. 98.

[5] *Ataque a la Embajada china: fue un error de información de la CIA*. Diario El Clarín. 1999 http://www.clarin.com/diario/1999/05/10/i-02801d.htm . Última consulta Noviembre 22 de 2008.

[6] BERKOWITZ, Bruce. Op. Cit. Pág. 98

[7] JARAMILLO, Carlos Eduardo. *Farc están cambiando de estrategia.* http://www.cambio.com.co/paiscambio/813/ARTICULO-WEB-NOTA_INTERIOR_CAMBIO-4780133.html. Revista CAMBIO. Última consulta Noviembre 22 de 2008.

"niebla de la guerra" como enuncia Clausewitz[8]. En las guerras de cuarta generación la niebla que se debe eliminar es el caos y la desinformación[9].

3. EL COMANDO, CONTROL Y COMUNICACIONES (C3) EN RED

Otro elemento tecnológico que ayudo a coordinar todas las acciones de la fuerza aérea de los diferentes países miembros de la coalición, fueron los denominados Centros de Comando, Control y Comunicaciones –C3 enlazados en red.

Una de las limitaciones con las que debía el gobierno de Estados Unidos lidiar era la voluntad política de cada unos de los países aliados, que de igual forma era llevado al terreno militar por cada uno de sus líderes militares. Para solucionar este problema se aprovecho la infraestructura del Centro de Comando de Estados Unidos (CENTCOM)[10].

El CENTCOM fue creado en 1983, con un área de acción limitada al oriente medio. El CENTCOM se encargó durante la Guerra del Golfo, de coordinar de manera conjunta todas las acciones militares que se desarrollaban. Las naciones miembros de la OTAN, no tuvieron mayor problema al trabajar de manera coordinada sobre una plataforma de comunicaciones común.

De esta forma las operaciones aéreas fueron dirigidas por la Fuerza Conjunta del componente del comando aéreo (JFACC), quienes se encargaban de seleccionar y valorar los blancos de manera conjunta con Inteligencia e igualmente seleccionar las armas que deberían de ser empleadas.

---

[8] SANCHEZ, Pedro. *Guerras de Cuarta Generación y las Redes.* Revista Ejercito No.812. Madrid. 2008. Pag. 15.
[9] Ibíd. Pag. 16.
[10] United States Central Command (USCENTCOM). http://www.centcom.mil/. Última consulta Noviembre 22 de 2008.

Los C3 se encargaron de concentrar la información bajada de los satélites meteorológicos, satélites espías, satélites de comunicaciones, y las trazas que reportaban los vuelos guiados por tecnología GPS.

Durante la guerra del golfo se destinaron 3 satélites permanentemente a facilitar las comunicaciones directamente desde el campo de batalla con el C3, de esta forma se garantizaba que la información que se obtenía del actuar del enemigo fuera concentrada en tiempo real en los centros de comando facilitando de esta forma la oportuna toma de decisiones.

La operación "Tormenta del Desierto", fue la primera guerra en la cuál el ejército americano operó usando un verdadero sistema de red de comunicaciones[11]. Este sistema enlazaba radios de comunicaciones, satélites militares y satélites comerciales. Este sería el preámbulo de las denominadas "ciberguerras", en las cuáles las unidades militares al estar intercomunicadas pueden actuar de manera simultánea y coordinada.

A partir de la guerra del golfo, se han desarrollado nuevas habilidades para la toma de decisiones basadas en información: La capacidad de neutralizar un adversario desde cualquier distancia con precisión, la capacidad de mantener vigilancia silenciosa sobre su enemigo y así poder aprovechar la oportunidad en que su adversario se torna débil y destruirlo, y finalmente la capacidad de administrar la eficientemente la información para tomar decisiones antes que su enemigo.[12]

Posterior a la guerra de golfo la tecnología informática siguió incrementado su capacidad de procesamiento de datos de manera exponencial. Paralelamente se presentó el fenómeno de la masificación del acceso a Internet y de la telefonía celular.

---

[11] BERKOWITZ, Bruce. Op. Cit., Pag. 71.
[12] BERKOWITZ, Bruce. Op. Cit. Pag. 75.

A principios de los años 90, Scott McNelly actuando como presidente de Sun Microsystems predice que los computadores permanecerán conectados a Internet[13]. A partir de esta premisa se crea el concepto de "guerras centradas en red"[14].

Este concepto adaptado a partir de la guerra del golfo, consiste en que cualquier embarcación, avión, vehículo o tropa pueda permanecer interconectado a la red de comunicaciones de defensa, intercambiando datos y colaborando de manera conjunta.

Nuevamente en la guerra de Irak en 2003, los comandantes de la operación planearon desde un comienzo una sola red integrada de comunicaciones apoyada en CENTCOM. Para poder operar de manera conjunta al ejército, armada y fuerza aérea en un modelo centrado en red[15].

Gracias a la tecnología de comunicación satelital se tiene la capacidad de estar dirigiendo las operaciones desde un centro de comando y control remoto. Disparar misiles desde plataformas de lanzamiento en los mares o países miembros de la coalición, sin tener que desplazarse hasta el sitio de combate.

Se generó entonces el concepto de "*despersonalización del combate*", que consiste en aprovechar las tecnologías de información y comunicaciones para disminuir las bajas en el ejercito amigo, y de manera precisa causar bajas y daños en el enemigo sin tener que entrar en luchas sangrientas frontales.

Adicionalmente se comenzaron a emplear las "*guerras electrónicas*", que interferían el espectro electromagnético de las ondas de radio que ayudarían a destruir el centro de comando y control iraquí. Aislando las tropas de invasión de su retaguardia en Bagdad.

---

[13] BERKOWITZ, Bruce. Op. Cit., Pag. 111.
[14] BERKOWITZ, Bruce. Op. Cit., Pag. 113.
[15] BERKOWITZ, Bruce. Op. Cit., Pag. 115.

Esta falta de los sistemas de C3 contribuyó al éxito de la campaña terrestre aliada. Irak no había contemplado esta debilidad, ya que en anteriores conflictos no se había presentado este tipo fallas y de igual forma no la tenían contemplada ya que sus vecinos árabes no poseían la capacidad para ejecutarla.

Las líneas de comunicación iraquíes estaban basadas en cables de fibra óptica, las cuáles fueron cortadas desde el principio del conflicto mediante el uso de operaciones de fuerzas especiales de Estados Unidos. La falta de comunicaciones digitales obligó al ejército iraquí a emplear sus radios de comunicaciones, que eran posteriormente interceptados, ubicados por las plataformas de inteligencia técnica y posteriormente destruidos.

Esta restricción a la capacidad de comunicaciones, le restó capacidad de movilidad a las fuerzas iraquíes reduciendo su efectividad para tomar decisiones y ejercer el mando y control de sus medios para el combate terrestre y aéreo.

Las tácticas sumadas al nuevo concepto de "*Dominio de la Información*", apoyado en las nuevas redes de comunicación satelital, le brindaron ventajas tácticas a los miembros de la coalición. Permitiendo en tiempo real tener un panorama de la misión en curso y de esta forma tomar mejores decisiones en menor tiempo.

"De ahí que luchar y conquistar en todas vuestras batallas
No es la suprema excelencia, la suprema excelencia consiste en
romper la resistencia del enemigo sin luchar"
Sun Tzu

4. LAS OPERACIONES DE INFORMACIÓN

La primera persona en mencionar el término "Guerra de información" fue Tom Rona en una monografía denominada "Sistemas de armas y Guerras de información", publicada en 1976. [16] Rona de manera visionaria afirma en su monografía, que las guerras de

[16] BERKOWITZ, Bruce. Op. Cit.,Pág. 30.

información ofrecen una gran ventaja sobre el adversario. Si se aprovechan la capacidad de controlar la información que fluye a través de las redes de comunicaciones y computadores del enemigo.

Posteriormente, las "guerras de información" se han presentado como un conjunto de herramientas y técnicas empleadas para garantizar el éxito militar a partir de la información y las ideas, en lugar de emplear las armas. Las guerras de información integran diversos aspectos de la guerra como el comando y control - C2, Inteligencia, guerra electrónica, guerra sicológica, guerras de información económica, ciberguerra y la intrusión en sistemas de cómputo.

Posterior a la guerra de Vietnam, el ejército de los Estados Unidos se encontraba en un proceso de reducción de personal y de recursos. Pero gracias a la guerra del golfo se reivindicó su poderío militar y aumentó la credibilidad y confianza del pueblo norteamericano.

Claro que todo esto, en parte se debe a la ejecución de una campaña de información que desvirtuaba a Sadam Houseim, y lo presentaba como un dictador al mismo nivel de Hitler. El cuál ordenó a finales de los años 80, acciones de limpieza étnica contra la población Kurda empleando gases[17].

Estas acciones previas al conflicto ayudaron a ganar la confianza del pueblo de los Estados Unidos en su ejército. Igualmente, ayudó a asegurar el apoyo de los aliados en la coalición para liberar Kuwait.

En la guerra, el nivel de la mente es de cierta forma el elemento que vincula la moral con lo físico. Es por eso que las operaciones sicológicas se encargan afectar la moral de los

---

[17] SANZ, Juan C. *El régimen de Sadam prosigue la 'limpieza étnica' contra los kurdos de Irak.* Diario El País. 2003. http://www.elpais.com/articulo/internacional/regimen/Sadam/prosigue/limpieza/etnica/kurdos/Irak/elpepiint/20030305elpepiint_4/Tes/ . Última consulta Noviembre 22 de 2008.

combatientes y del pueblo que los apoya. Para lograr afectar y disminuir las acciones físicas por parte del enemigo.

Aplicando estrategias de las guerras de cuarta generación y apoyándose en los desarrollos tecnológicos. Se aprovecharon los mensajes emitidos por lo medios de comunicación para influir en la opinión pública. Demostrando como la propaganda previamente y durante los momentos de guerra, puede ser empleada como un arma estratégica y operacional.

De esta forma, es como la televisión fue empleada en Vietnam para transmitir las escenas de horror que se cometían durante el conflicto. Pero el momento de partida de las transmisiones en vivo de las guerras, se logró durante la guerra del golfo.

Esto generó los historiadores denominan "*el efecto CNN*", nombre dado gracias a la cadena de televisión que transmitió en vivo a todo el mundo los bombardeos empleados por fuerzas de la coalición.

La Guerra del Golfo fue la mayor guerra transmitida en vivo, por lo medios de comunicación a la opinión pública. Desde el primer día de la ocupación a Kuwait, el ejército de los Estados Unidos implementó operaciones sicológicas para controlar la forma de cómo presentar la guerra al mundo.

Organizaciones de la prensa como CNN comenzaron a trasmitir en vivo las 24 horas la forma como los misiles guiados por láser afectaban a las ciudades de Bagdad, Tel Aviv, y Riyadh[18]. Los militares de los Estados Unidos presentaron ciertos resquemores a las transmisiones en vivo ya que podrían afectar la estrategia y la táctica empleada.

---

[18] DEPARTMENT OF THE NAVY - NAVAL HISTORICAL CENTER. *War Chronology: January 1991.* http://www.history.navy.mil/wars/dstorm/dsjan2.htm . Última consulta Noviembre 22 de 2008.

Sadam Houseim hábilmente aprovechó estas trasmisiones en directo que mostraban los efectos que causaban los bombardeos sobre la población civil de Bagdad, con propósitos de propaganda para ganar apoyo de la comunidad mundial para su causa.

A partir de la selección de blancos precisos para ser bombardeados con ayuda de los proyectiles inteligentes Tomahawk, se creo un nuevo concepto de guerra denominado "Guerra Quirúrgica"[19]. Se hizo creer a la opinión pública que todas las operaciones fueron quirúrgicas al impactar los misiles sus blancos, sin causar daños colaterales.

En algunos casos los medios de comunicación fueron censurados por parte de la coalición, para no informar de ciertos errores de precisión en los bombardeos[20]. Solo al terminar la guerra se supo que el 90% de los misiles disparados no eran guiados por láser y en su mayoría no alcanzaron lo blancos identificados por inteligencia. De igual forma los misiles Patriot lanzados por Israel para interceptar los misiles Scuds, lanzados por Irak sobre Israel causaron algunos daños sobre la misma población de Israel.

Posterior a la Guerra del Golfo y como consecuencia del uso masivo de las tecnologías de información, los militares han perdido cada vez más su capacidad de censura de la información gracias a Internet.

Estados Unidos como tácticas sicológicas, aprovechó el espectro electromagnético programando emisoras de radio 18 horas al día. Con el objetivo que la población civil y los combatientes escucharan solo los mensajes que la coalición quería que recibieran. Se aseguraron de tal forma que dejaron caer radios programados solo en la frecuencia en la cual se escuchaban los mensajes emitidos por los aliados[21].

---

[19] ROGERS, A.P.V. *Una guerra sin víctimas*. Revista Internacional de la Cruz Roja No. 837. 2000. Pág. 165. http://www.icrc.org/web/spa/sitespa0.nsf/html/5TDNZD. Última consulta Noviembre 22 de 2008

[20] ALBARRÁN, Gerardo. *La guerra mediática*. Sala de Prensa. http://www.saladeprensa.org/art283.htm. Última consulta Noviembre 22 de 2008.

[21] GOLDSTEIN, Frank I. *Las Operaciones Psicológicas la Guerra del Golfo Pérsico*. Air & Space Power Journal.1996. http://www.airpower.au.af.mil/apjinternational/apj-s/1996/3trimes96/goldstein.html. Última consulta Noviembre 22 de 2008.

A los prisioneros de guerra iraquíes se les presentaban películas elaboradas de acuerdo a las leyes musulmanas, pero ellos preferían ver películas de la cultura norteamericana como "*Superman*".

Fueron diseñados cerca de 29 millones de panfletos con propaganda, que fue esparcida sobre Irak[22]. Estos panfletos fueron diseñados lo más simple posible, asumiendo que los soldados iraquíes tenían una educación muy básica. La coalición posteriormente hacia caer estos volantes sobre la infantería iraquí donde advertían que al siguiente día a la misma hora se efectuaría un bombardeo. Posterior al ataque se difundía la noticia por la radio de la coalición, garantizando de esa forma la credibilidad por parte de las fuerzas invasoras de Kuwait[23].

En los volantes desplegados por la coalición se presentaban imágenes que mostraban a soldados americanos efectuando desembarcos anfibios en las costas, los cuáles nunca se realizaron. El ejército de Irak creyó que un asalto por las costas de Kuwait se llevaría a cabo, con el propósito de que las tropas iraquíes orientaran sus tropas a proteger la región costera.

Se estima que de los 300,000 hombres del ejército iraquí, cerca del 98% de ellos leyó los panfletos y un 88% de las tropas se consideró influenciado por la combinación de las operaciones sicológicas, la campaña aérea y la campaña terrestre[24].

La propaganda iraquí de su parte se encargaba de exaltar el nacionalismo, la religión y a su líder Saddam Hussein. Es así como el Ministerio de cultura e información aplicó el modelo soviético de propaganda orientado a justificar la invasión de Kuwait, obtener el apoyo de la población árabe, tratar que las naciones que hacían parte del embargo desistieran de seguir haciéndolo e impedir acciones militares sobre Irak. Se difundieron varios rumores sobre el bien preparado y numeroso ejército iraquí, cosa que resultó falsa en la práctica.

---

[22] Ibíd.
[23] Ibíd.
[24] Ibíd.

CONCLUSIÓN

Uno de los errores cometidos por Sadam Houseim, fue el de seguir rígidamente la doctrina y no ser capaz de innovar.

Error que fue explotado por la coalición al convertir la Guerra del Golfo en una guerra asimétrica, en la cuál poder explotar sus nuevas tecnologías. Aprovechar los sistemas de vigilancia remotos para ubicar y monitorear las posiciones de las fuerzas iraquíes. Cortar sus líneas de fibra óptica para obligarlos a usar los medios de comunicación que podían ser monitoreados. Atacar los centros de comando, control y comunicaciones al comienzo de la operación, para que las tropas invasoras iraquíes se sintieran aisladas y vulnerables ante las operaciones sicológicas de la coalición. Transmitir en vivo a todo el mundo el conflicto, ayudó a crear una imagen de confianza del pueblo americano y de los países miembros de la coalición en los Estados Unidos.

La tecnología militar al final logró salir triunfadora, gracias al ingenio de los líderes militares de la coalición. Las nuevas tecnologías de información y comunicaciones fueron empleadas acertadamente en el campo de acción para el cuál fueron diseñadas.

El autor Alvin Toffler dice "... las innovaciones tecnológicas añadieron nuevos elementos o crearon combinaciones diferentes de elementos antiguos dentro de un juego existente, pero una verdadera revolución va mas allá: cambia el propio juego, incluyendo sus reglas, sus medios, el volumen y la organización de los equipos, su adiestramiento, doctrinas, tácticas y simplemente todo lo demás. "[25] Se podría interpretar que aunque la naturaleza de la guerra no cambia, el uso de las tecnologías militares implica adaptaciones en la forma de tomar decisiones políticas y operacionales.

De igual forma Adams en su libro "La próxima guerra mundial" dice que "La revolución tecnológica que atraviesa la sociedad, impacta directamente sobre sus militares, por lo tanto

[25] TOFFLER, Alvin y Heidi, *Las guerras del futuro*, Editorial Plaza & Janes, 1998.

es ilógico no pensar que los adelantos tecnológicos seguirán impactando en la forma de combatir y de planear la guerra por parte de los ejércitos de esas sociedades"[26]. Los actuales y futuros estrategas siempre han tenido la información como un insumo para la tomas de decisiones. A principios del siglo XX se consideraban tres teorías que competían por el poder militar: tierra, mar y aire. En el siglo XXI aparece un cuarto poder y es dominio de los sistemas electrónicos de información[27].

Esta guerra sirvió para probar varias de los nuevos conceptos que hoy se aplican en las guerras denominadas de cuarta generación[28]. Según el coronel John Boyd, en las guerras se debe tener en cuenta tres niveles: Moral, Mental y Físico. Las nuevas tecnologías se usaron para minar la moral y la mente de las tropas de Irak y de su pueblo, así como en el campo físico para anular sus activos estratégicos.

La Guerra del Golfo presentó al mundo entero el comienzo de las nuevas formas y medios de guerra por parte de las superpotencias como Estados Unidos y sus aliados. Esta guerra sirvió para marcar un cambio significativo en el empleo de las nuevas tecnologías de información y comunicaciones para ganar los conflictos, en coordinación con formas de operaciones conjuntas y coordinadas.

En el caso de Colombia gracias a la cooperación militar con los Estados Unidos y la dinámica del conflicto interno, ya se han evidenciado el uso de las tecnologías de información y comunicaciones. Tal es el caso, de las bombas inteligentes empleadas en operaciones contra cabecillas de las FARC, como el "Negro Acacio" y "Raúl Reyes".

Operaciones de información en Internet como la empleada en la operación Jaque, donde a las FARC se les hizo crear que la organización "Misión Internacional Humanitaria" era

---

[26] ADAMS, K. *La próxima guerra mundial*, Editorial Granic, Madrid, 2001
[27] BERKOWITZ, Bruce. Op. Cit. Pag. 183.
[28] LIND, William S. *Fourth Generation Warfare: Another Look.* http://www.d-n-i.net/fcs/4GW_another_look.htm. Última consulta Noviembre 22 de 2008.

real. Acudiendo al método de montar una página oficial de la misión en Internet que se encontraba hospedada en la dirección http://misionhi.org/ [29] .

Las fuerzas militares en Colombia, ya han comenzado a adaptar su organización para operar de manera conjunta y próximamente con centros de Comando, Control y Comunicaciones unificados entrelazados en red.

[29] ALBON, Chris. *Colombian Hostage Rescue Could Have Been Foiled By A Single Internet Search*. 2008. http://warandhealth.com/colombian-hostage-rescue-could-of-been-discovered-by-a-single-internet-search/ . Última consulta Noviembre 22 de 2008.

CAPÍTULO II

COMANDO, CONTROL Y COMUNICACIONES: UNA HERRAMIENTA CLAVE EN LA ESTRATEGIA MILITAR

> "El comando y control efectivo le asegura al comandante la habilidad de sincronizar las acciones de sus unidades en el tiempo correcto, el lugar adecuado, con el propósito indicado para asegurar la unidad del esfuerzo...y todo esto implica el cumplimiento de la misión de la manera más efectiva posible[30]"

INTRODUCCIÓN

Los comandantes a través de la historia siempre han tomado decisiones en medio de la "niebla de la guerra" como lo sugiere Clausewitz. Lo anterior implica disponer de herramientas que permitan dar claridad al panorama operacional y evaluar permanentemente la estrategia. En la era de la información los sistemas de comando, control y comunicaciones (C3) ayudan a minimizar la incertidumbre y las fricciones propias de la guerra, contribuyendo a aumentar el poder operacional y táctico.

Con el advenimiento de los sistemas de comunicaciones digitales, los comandantes soportan sus decisiones en los sistemas de comunicaciones para conducir sus operaciones. Y de esta forma ejercer las funciones de dirección y ejecución adecuadamente, gracias a que pueden enviar sus órdenes oportunamente a sus unidades de maniobra, apoyo y logística.

A partir de la Guerra del Golfo los sistemas de comando, control y comunicaciones han evolucionado hacia redes interconectadas de manera igual como opera Internet. Este nuevo modelo de operaciones centradas en red, permite a todas las personas o entidades involucradas en una operación conocer en todo momento la información que aporta cada

---

[30] CRAIG, Deare. *Panel: Mexico and the Hemispheric Security Agenda. El Comando Norte de los Estados Unidos Implicancias para la Seguridad y Defensa de México.* Center for Hemispheric Defense Studies. 2003.

una de ellas a la red de conocimiento militar. Y de esta forma, ayudar a todos los participantes a crearse un panorama de la situación a nivel táctico, operacional y estratégico según sea el nivel en que opere.

El propósito de este capítulo es el de presentar como en la Era de la Información los sistemas de comunicaciones digitales han permitido considerar a los centros de comando, control y comunicaciones, como una herramienta clave que ayuda al éxito de las estrategias militares de los ejércitos del siglo XXI.

Igualmente presentar el caso del comando, control y comunicaciones en la Fuerza Armadas colombianas, y como actualmente se encuentran en un proceso de modernización gracias a la dinámica del conflicto interno.

1. EVOLUCION DEL COMANDO, CONTROL Y COMUNICACIONES

El término *Comando* ha sido usado por miles de años y C2 solo ha sido usado más de medio siglo. Diferentes autores han desarrollado las siguientes definiciones de Comando y Control:

- C2 es el término común en lenguaje militar para la administración de personal y recursos[31].
- Comando comprende la responsabilidad para usar efectivamente los recursos disponibles, planeando el empleo de, organizando, dirigiendo coordinando y controlando las fuerzas militares para el logro de las misiones asignadas[32].
- Comando es la expresión creativa de la voluntad humana necesaria para ejecutar la misión. Control son las estructuras y procesos concebidos por el comando para habilitarlo y para administrar el riesgo[33].

---

[31] ALBERTS, David S. Hayes, Richard E.. *Command Arrangements for Peace Operations*. Washington, DC. CCRP Publication Series. Pág. 5.

[32] *Unified Action Armed Forces.* Washington, D.C., Joint Pub,1995.

Al parecer en la II guerra mundial se comenzó a usar el término C2[34] cuando se comenzaron a emplear las operaciones combinadas y conjuntas cuando el comando tuvo que cruzar las fronteras de los países.

Antes de los 70's C2 fue poco usado y se hablaba en su lugar del estado mayor, debido a que eran los responsables de las tareas operacionales y administrativas. Aunque comandantes como Alejandro Magno y Cesar no tenían estado mayor, ellos hacían este trabajo por si mismos. Napoleón comando sus grandes ejércitos con unos cuantos subordinados. Sin embargo, estos comandantes necesitaron de las comunicaciones y la inteligencia para complementar las tareas de Comando y Control.

Existen algunas definiciones que enmarcan el *Comando* como un arte y el control como una ciencia y el comandante en el Comando y el Estado Mayor en el *Control*, pero en las guerras modernas el Comando y control es una responsabilidad distribuida.

Antes de la era industrial los comandantes tomaban sus decisiones de maneras individuales y basadas en su percepción de la situación[35]. Alejandro Magno ejercía un control fuerte y centralizado de sus tropas, el cuál usaba para direccionar sus campañas sin consultar a sus subalternos.

Recurría a su experiencia y conocimiento del enemigo, para direccionar su estrategia. Se ubicaba en una posición dominante para visualizar sus propias tropas y las del contrincante. En persona daba órdenes a sus tropas, y también combatía en campaña.

Se puede así evidenciar que el factor clave del control de estas fuerzas, fueron las habilidades militares y de liderazgo del comandante.

---

[33] ALBERTS, David S. Hayes, Richard E. *Power to the Edge. Command...Control...in the Information Age.* Washington, DC. CCRP Publication Series.
[34] SPROLES, Noel. *Establishing Measures of Effectiveness for Command and Control: A Systems Engineering Perspectiva.* University of South Australia.2001.
[35] KEEGAN, John. *The Mask of Command*, Penguin Books, 1987.

La creación de grandes ejércitos en el siglo XVIII, hizo que el Control se centralizara en estructuras jerárquicas. El ejército Prusiano fue el primero en crear el Estado Mayor como apoyo a la cadena de mando y así incrementar el control[36]. Fue de esta forma que los comandantes comenzaron a requerir información de sus subalternos para una mejor toma de decisiones, ya que sus tropas se encontraban dispersas.

Federico el Grande fue uno de los primeros en ubicar su cuartel general en la retaguardia, comenzando a tomar sus decisiones basado en la información que recibía de los líderes de sus tropas. Este concepto según Clausewitz es denominado el "reino de la incertidumbre"[37].

En el siglo XIX la introducción de nuevas tecnologías generó un cambio de nuevo en la forma de control. La introducción del tren permitió la movilidad de grandes ejércitos. El telégrafo permitió un mayor control centralizado por parte de los comandantes, sobre las fuerzas ubicadas a gran distancia. Esto hizo que el tiempo en la toma de decisiones se redujera significativamente.

Antes de la introducción del ferrocarril en 1840, enviar una página de texto se demoraba varios días o semanas, con la llegada del ferrocarril se demoraba unos pocos días. Luego con invención del telégrafo unos minutos, y posteriormente con la invención del correo electrónico se demora segundos en llegar a sus destinos[38].

La reducción de los tiempos para que los comandantes tuvieran la información en sus manos, generó que tuvieran un mayor control centralizado y adicionalmente comenzaron a ser dependientes de las nuevas tecnologías de comunicaciones. De esta forma los

---

[36] CREVELD, Martin. *Command in War*, Cambridge. Howard University Press, 1985.
[37] HOWARD, Michael. Paret, Peter. *Carl von Clausewitz: On War.* Princeton, NJ. Princeton University Press, 1989, página 101.
[38] YATES, Benjamin. *The past and present as a window on the future.* New York. Oxford University Press. 1991.

comandantes confiaban cada vez más en la tecnología de la información para reducir "el reino de la incertidumbre" como lo describió Clausewitz[39].

Con el propósito de reducir la incertidumbre de la guerra, algunos comandantes en el nivel más alto de jerarquía tienden a orientar su organización hacia un control centralizado. Generando un efecto que al tener menos incertidumbre en la cima de la organización, genera más incertidumbre en los niveles bajos. Reduciendo de esta forma la autonomía de los comandantes en el campo de batalla para la toma de decisiones[40].

Las tecnologías de la información y comunicaciones brindan la capacidad para que los comandantes que toman decisiones estratégicas, se vean involucrados en las decisiones al nivel táctico. Esta capacidad que proveen las redes de comunicaciones de permitir al comandante comunicarse con las tropas en combate, generó un cambio dramático en Comando y Control. Esto se vio reflejado en el incremento del uso de los radios en la II guerra mundial, en Vietnam y luego en tormenta del desierto.

En la era de la información los tiempos para la toma de decisión en las operaciones es cada vez mas corto, llegando al tiempo real como se puede observar en el siguiente cuadro comparativo:

	Guerra Revolucionaria	**Guerra Civil (USA)**	**II Guerra Mundial**	**Guerra del Golfo**	**Guerras Del Futuro**
Observar	Telescopio	Telégrafo	Radio/Cable	Cerca del Tiempo Real	Tiempo Real
Orientar	Semanas	Días	Horas	Minutos	Continua
Decidir	Meses	Semanas	días	Horas	Inmediata
Actuar	1 estación	1 Mes	1 Semana	1 Día	Menos de una hora

Tabla 1. Evolución de los tiempos para completar el ciclo para la toma de decisiones[41]

[39] HOWARD, Michael. Op. Cit.
[40] ROMAN, Gregory A. *The Command or Control Dilemma: When Technology and Organizational Orientation Collide.* Air War College Maxwell .1996. Pág. 11.
[41] Ibíd.

En los conflictos actuales gracias a las nuevas tecnologías de la era de la información, el comandante tiene la capacidad de mando, control y comunicaciones (C3) a velocidades y exactitud nunca antes vistas. Contribuyendo de esta forma al éxito operacional, gracias a la información precisa y oportuna que brinda el centro de comando y control[42].

Desde mediados del siglo XX se han venido presentando el cambio de los conflictos de guerra regular hacia guerras asimétricas, que han implicado replantear y modernizar los modelos estratégicos, operacionales y tácticos. Por lo cuál se ha vuelto cada día más común el desarrollo de operaciones conjuntas a manera de coaliciones entre países u operaciones conjuntas entre fuerzas del mismo país, implicando un incremento en la complejidad de las operaciones militares.

Este incremento de la complejidad de las amenazas y operaciones hace necesario cambiar la modalidad de mando y control, pasando de la era industrial hacia la era de la información en el siglo XXI.

Los líderes requieren para conducir sus operaciones de los sistemas de comunicaciones que les ayudan a ejercer las funciones de dirección y ejecución gracias a que pueden enviar sus órdenes oportunamente a sus unidades de maniobra, apoyo y logística. Estas nuevas facilidades llevarán a que las fuerzas armadas reestructuren su organización, entrenamiento, uso y procesos de negocios.

El comando y control (C2) se ha ido expandiendo hacia las Comunicaciones(C3), Computadores (C4), Inteligencia (C4I), Información (C4I2), en la fuerza aérea se expande a Investigación y Reconocimiento (C4ISR), quizás un siguiente paso sea Coordinación (C5I2) o Cooperación (C6I2) implicando cada uno la adopción de una nueva tecnología[43].

---

[42] CRAIG A, DEARE. Op. Cit.
[43] TODD, Greg. *C1 Catharsis*. Army War College, 1986, Pág. 14.

El ejercito y la armada del siglo XXI gracias a las tecnologías de la información verán la descentralización del comando y control, y la fuerza aérea verá la oportunidad de tener un control centralizado ya que la dimensión del espacio aéreo así lo requiere[44].

Las fuerzas armadas del siglo XXI tendrán como reto aprovechar las ventajas estratégicas que presenta la era de la información, ante los modelos actuales de organizaciones regidas aún por la era industrial.

El Comando y Control (C2) en el siglo XXI en los escenarios de guerras regulares y asimétricas, ha comenzado a evolucionar y adaptarse para aprovechar las facilidades que brinda la era de la información. Es así como ha ido evolucionando hacia modelos de operaciones centradas en redes.

Sin embargo, la información y la tecnología no lo es todo sin el factor humano que se encarga de dirigir y orientar las operaciones militares. Así mismo, la conciencia situacional de los comandantes es necesaria para evaluar y valorar el escenario del campo de batalla.

2. EVOLUCION DEL COMANDO, CONTROL Y COMUNICACIONES HACIA EL MODELO DE OPERACIONES CENTRADAS EN RED

El comando y control como todo proceso que hace parte de la estrategia militar operacional esta encaminado a conducir al cumplimiento de unos objetivos, producto de una serie de acciones u operaciones.

Este proceso se puede enmarcar en un ciclo de Observar, Entender, Orientar, Decidir y Actuar[45]. Proceso conocido como el ciclo de Boyd, en honor a su creador Jhon Boyd.[46]

---

[44] BARNETT,Jeffery R. *Future War: An Assessment of Aerospace Campaigns in 2010.* Air University Press, 1996. Pág. 33.

[45] SPROLES, Noel. *Command and Control as a process. Establishing Measures of Effectiveness for Command and Control: A Systems Engineering Perspectiva.* University of South Australia Study. 2001.

[46] Ibíd.

Consiste en tener los mejores datos de la situación operacional en que se encuentre el comandante de una misión. Luego evaluar los datos contra el conocimiento previo de su enemigo, escoger el mejor curso de acción y ejecutarlo[47].

En el curso de una operación militar el comandante toma decisiones, reparte instrucciones, observa y evalúa los resultados, y vuelve a tomar decisiones basado en la retroalimentación producto de sus anteriores acciones. El control se encarga de observar los resultados y producto de ello mejorar o cambiar decisiones previas para cumplir las ordenes.

El comandante se apoya en datos y reportes que traen información del enemigo y de sus propias tropas para Observar, al relacionar estos datos se genera información para crear el mapa mental de la situación y así poder Entender y Orientar la situación. Entender las situaciones y la mente del enemigo es una de las más valiosas habilidades de los grandes generales. Después de Orientar el comandante es capaz de Decidir como Actuar para poner el plan trazado en marcha, de nuevo el comandante es capaz de observar los resultados producto de sus decisiones y de nuevo comienza el ciclo del Comando y Control.

Este proceso se ve afectado por lo que denomina Clausewitz como la "niebla de la guerra" debido a que el factor humano hace parte de este proceso.

Durante el período de la guerra fría los soviéticos gracias al fortalecimiento de sus sistemas de comunicaciones pudieron adaptar su propio concepto de comando y control[48]. El cuál consistía en que cada unidad sabía su papel, en cada paso dentro de la operación y lo practicaba una y otra vez. Permitiendo a los comandantes controlar de manera predictiva el comportamiento de sus fuerzas y medir su progreso basado en su entrenamiento.

---

[47] BERKOWITZ, Bruce. Op. Cit. Pág. 42.
[48] RICE, Condoleezza. *The Party, the Military, and Decision Authority in the Soviet Union.* World Politics. Vol. 40, No. 1. 1987. Pág. 55-81.

En la era de la información, las amenazas difieren de las de la era industrial. Muchas de ellas no se pueden atacar con tácticas militares convencionales, por lo cuál los C2 requieren implementar los principios de Interoperabilidad y Agilidad.

El resultado de la interoperabilidad se puede describir en una simple frase "Todo el mundo necesita hablar con todo el mundo", de esta forma las organizaciones ágiles serán capaces de enfrentar retos inesperados y llevar a cabo tareas de nuevas formas.

Los nuevos enfoques en comando, control y comunicaciones han hecho replantear los esquemas jerárquicos de las comunicaciones, a redes robustas y eficientes basadas en la interconexión de nodos de los cuáles algunos de ellos tienen más capacidad de transmisión que otros, y a su vez estos sirven de puente de conexión con otros nodos de la red. Este esquema de conexión de nodos a manera matricial, es el esquema eficiente en el cual se basa Internet.

La visión de operaciones centradas en red, consiste en que cualquier persona, en cualquier lugar podrá acceder a cualquier fuente de información y la podrá explotar siempre que tenga el nivel de acceso necesario.

La tarea es proveer conectividad a toda la organización desde el nivel táctico, pasando por el operacional y llegando al nivel estratégico. Esto incluye a las tropas en terreno, los vehículos de combate, los centros de comando, las aeronaves y las embarcaciones de combate. Cada unidad ve las suma de lo que las otras unidades ven, y al reunirse la información en red aumenta la conciencia situacional del teatro de operaciones lo cual resultará en una planeación estratégica mas rápida y decisiones tácticas mas efectivas.

Este concepto de permitir una red de comunicaciones integrada se base en la Ley de Metcalfe, la cuál dice que el valor potencial de una red incrementa exponencialmente (n^2) a

partir del número de participantes (n) en la red[49]. Las personas que participan en los procesos en red, deben tener toda la capacidad de conexión e interoperabilidad para que al contribuir a los procesos de decisión aumente el valor de la red en la que colaboran.

Es así como la habilidad de representar y explorar el enfoque de Comando y control (C2) y los nuevos conceptos de comando centrados en redes, se han convertido en una de las prioridades para la modernización de la defensa de las naciones en la era de la información[50].

Las operaciones militares que apliquen el nuevo enfoque basado en operaciones centradas en red, mejorarán los conceptos de maniobra, precisión en los combates y la logística gracias a la superioridad en la información.

3. EL PAPEL DEL COMANDO Y CONTROL Y COMUNICACIONES EN LA FFMM DE COLOMBIA.

> "Soldados de tierra, mar y aire: el compromiso que hemos adquirido con el pueblo colombiano demanda el fortalecimiento de unas herramientas esenciales, enmarcadas dentro de una doctrina conjunta que facilite el liderazgo requerido para la conducción de unas fuerzas militares limitadas en recursos, eficaces y transparentes y pletóricas de gloria al servicio del pueblo colombiano." General Freddy Padilla de León.

Las fuerzas militares de Colombia han sido líderes en la aplicación de políticas de unificación del mando desde 1944 cuando se crea la figura de Jefe de Estado Mayor, y posteriormente en 1951 creó el cargo de Comandante General con las funciones de mando de las Fuerzas Militares[51].

---

[49] ALBERTS, David S. *Network centric warfare : developing and leveraging information superiority*. Washington, DC. CCRP Publication Series. 2000. Pág. 250.

[50] NORTH ATLANTIC TREATY ORGANISATION. *Exploring New Command and Control Concepts and Capabilities*. www.rta.nato.int. 2007. Última consulta Noviembre 22 de 2008.

[51] VARGAS, Alejo. *Las fuerzas armadas en el conflicto colombiano. Antecedentes y perspectivas*. Bogotá. Intermedio Editores. 2002. Pág. 441.

En el mismo año de la creación del cargo de Comandante General, Colombia decide apoyar a las Naciones Unidas en la Guerra de Corea. Gracias a la participación de los soldados del batallón Colombia, se logró capitalizar el conocimiento que adquirieron al estar bajo el mando y entrenamiento del ejército de los Estados Unidos.

Cuando estos oficiales y suboficiales se reincorporaron de nuevo a sus labores en Colombia, trajeron consigo nuevas técnicas y tecnologías de comando, control y comunicaciones. Desde esos días las fuerzas armadas comenzaron un proceso de modernización de los sistemas de comunicaciones para facilitar las maniobras de los comandantes.

Durante la evolución del conflicto interno en Colombia, es oportuno recordar como alias "Tiro Fijo", actuando como comandante de las FARC en los años 90s gracias a las radiocomunicaciones, y el dominio y control de posiciones estratégicas. Podía sin ningún problema, hacer programas radiales con mas de cien (100) de sus comandantes sin ser ubicado.

Este esquema se fortaleció aún más cuando se creo la "zona de distensión" donde se concentró el comando central en una posición segura, desde la cuál se podía orientar y controlar los combatientes de las FARC. Convirtiéndose esta fortaleza en uno de los objetivos a ser atacados como parte de la estrategia militar operativa del ejército colombiano, posterior a la zona de conflicto.

En el período comprendido entre 1999 y 2002, las Fuerzas Armadas impulsaron cambios tecnológicos en los campos de la planeación y conducción de las operaciones militares, las estructuras de comando, control y comunicaciones[52]. Con el objetivo de contrarrestar los reveses sufridos por las Fuerzas Armadas colombianas en los años 90s.

---

[52] Fundación Seguridad y Democracia. *Fuerzas Militares para la guerra. La agenda pendiente de la reforma militar.* Bogotá, 2003. Pág. 56.

Las Fuerzas Armadas actualizaron sus sistemas de comando, control y comunicaciones a nivel del Comando General de las Fuerzas Militares, y a nivel de cada una de las fuerzas[53]. Se cambio el sistema de repetidoras por el de comunicaciones satelitales en el nivel estratégico. Aunque actualmente a nivel táctico se conserva el sistema de repetidoras a través de la Red Integrada de Comunicaciones (RIC)[54].

Gracias a este primer proceso de modernización tecnológica, se puede afirmar que hoy día las fuerzas militares colombianas cuentan con un sistema de Comando, Control, Comunicaciones, que le permite a nivel estratégico conducir operaciones[55].

Las Fuerzas Armadas paralelamente, han implementado una serie de cambios institucionales y doctrinarios como la creación de comandos conjuntos que han permitido implementar y aprovechar las nuevas tecnologías[56].

Las FFMM de Colombia adoptaron en algunos períodos de la historia la creación de comando unificados como el Comando Unificado del Sur (CUS), el Comando Unificado de Oriente (CUO) y el Comando Específico de San Andrés y Providencia (CESYP); todos estos con una misión definida e integrados por componentes de las diferentes Fuerzas[57].

Estas experiencias de comandos unificados no habían generado tanto impacto en la estrategia operativa de la guerra contra la subversión, como lo causó la creación en el año 2003 de la Fuerza de Tarea Conjunta Omega. Fuerza donde el Ejército, Armada y Fuerza Aérea unificaron esfuerzos sobre la retaguardia estratégica de las FARC.

En el año 2004 se creó el Comando Conjunto No. 1 "CARIBE", con el propósito de coordinar operaciones conjuntas entre las diferentes Fuerzas en la zona norte del País.

---

[53] Ibíd. Pág. 57.
[54] Ibíd. Pág. 75.
[55] Ibíd.
[56] Ibíd. Pág. 59.
[57] BARRERA H., Guillermo. La *importancia de las operaciones conjuntas, coordinadas y combinadas de la Armada Nacional*. http://www.armada.mil.co/?idcategoria=537943. Última consulta Noviembre 22 de 2008.

Actualmente se habla de un nuevo Comando Conjunto, el del Suroccidente, que tendrá sede en Tumaco y unirá a todas las fuerzas que operan en el área.

Los éxitos logrados por estos comandos conjuntos apoyados por el comando y control unificado, ha incrementando el poder de combate. Han contribuido entre otros éxitos a que los narcoterroristas de las FARC hayan perdido gran control sobre el territorio que antiguamente dominaban. Generando indisciplina táctica y pérdida de mando y control sobre las unidades de las FARC[58].

CONCLUSIÓN

Las FFMM de Colombia gracias a los cambios estructurales que ha implementado a través de los comandos conjuntos, demuestra como un cambio en los esquemas de mando y control a nivel estratégico operacional pueden generar resultados exitosos.

Este modelo de comandos conjuntos es el escenario ideal para la implementación de centros de comando, control y comunicaciones, para lograr que los comandantes tengan una visión panorámica de las misiones que se desarrollaran dentro del teatro de operaciones bajo su mando.

Es recomendable para Colombia continuar con el proceso de fortalecimiento y modernización de los sistemas de comando, control y comunicaciones. No solo para el conflicto interno, sino para la defensa de la nación en caso de conflictos internacionales.

Las operaciones realizadas contra las FARC durante el período de la política de seguridad de democrática del actual gobierno, demuestran como al atacar los sistemas de comando, control y comunicaciones, de este grupo narcoterrorista se disminuye su poder operacional y de maniobra.

---

[58] Ministerio de Defensa Nacional. *Las FARC en el peor momento de la historia.* http://www.mindefensa.gov.co/descargas/Documentos_Home/Farc_el_peor_momento_de_la_historia.pdf. Última consulta Noviembre 22 de 2008.

Finalmente se presentan a continuación las ventajas que aporta a la estrategia militar operativa, el empleo para Colombia de las tecnologías de comunicaciones en red. En concordancia con los nuevos modelos de comando, control y comunicaciones:

- Los comandantes vía video conferencia reducen el tiempo de planeación y eliminan a cero los tiempos que se empleaban en desplazamiento. Incrementando de esta forma el poder de combate, ya que anteriormente los comandantes de división se tenían que desplazar hasta los campos de batalla para planear el combate.
- Los especialistas pueden brindar sus servicios desde sitios centrales donde se concentra la información gracias a la red de datos. Logrando disminución de costos y aumentando el capital intelectual pudiendo capitalizar las lecciones aprendidas. Incrementando el poder operacional, ya que anteriormente se debían desplazar especialistas hacia el teatro de operaciones.
- Gracias al correo electrónico, video conferencia, telefonía satelital las tropas pueden permanecer en contacto con sus familias. Incremento el poder operacional, e igualmente incrementando un intangible que es la Moral de las tropas.
- Empleando la videoconferencia y la Intranet las unidades pueden capacitarse sin tener que desplazarse y en el horario que más les convenga. En Colombia un ejemplo de ello es el convenio establecido entre las FFMM el SENA y la Agenda de conectividad. Incremento el poder operacional y de la moral de las tropas.
- Los comandantes pueden coordinar y planear de manera colaborativa, reduciendo significativamente los tiempos de alistamiento para el combate. Incrementando el poder de combate a nivel táctico.
- Las tropas llevan equipos de GPS que envían su ubicación en tiempo real al centro de comando y control permitiendo una mayor capacidad de maniobra de las tropas y disminuyendo la posibilidad de fuego amigo. Incrementando la capacidad operacional y del poder de combate.

CAPÍTULO III

LA NECESIDAD DE DISEÑAR PARA COLOMBIA UNA ESTRATEGIA DE SEGURIDAD NACIONAL PARA LA PROTECCION DEL CIBERESPACIO.

"Si utilizas al enemigo para enfrentarlo,
serás poderoso en cualquier lugar a donde vayas."
Sun Tzu

INTRODUCCIÓN

Hace unos años se decía que la nación que tenga la información tenía el poder, pero este concepto ha cambiado, para decir que la nación que tenga la información y la capacidad para usarla en su favor tendrá el poder.

Colombia como un país en desarrollo y participe del proceso de globalización no se ha aislado del fenómeno de las redes interconectadas de datos como Internet.

Los usuarios de Internet en América Latina alcanzaron para marzo de 2008 los 104 millones de usuarios y una penetración del 27.1%. Colombia tiene 13 millones de usuarios y penetración de 30.5%, Perú con 7 millones de usuarios y 26% de penetración, Venezuela con 6 millones de usuarios y 23% de penetración, Ecuador tiene 1 millón de usuarios y penetración del 8%, Cuba tiene 240,000 usuarios con una penetración del 2,1% y Nicaragua con 155,000 usuarios con penetración del 2.7%, y países como Estados Unidos tiene un nivel del 72.5% de penetración[59].

Las anteriores cifras ayudan a ilustrar como cada año Colombia depende más de las redes de comunicaciones basadas en Internet, al igual que sus telecomunicaciones, banca, y medios de comunicación (Prensa escrita, Radio, TV).

---

[59] *SOUTH AMERICA*. http://www.internetworldstats.com/south.htm . Última consulta Octubre 7 2008.

Este capítulo pretende demostrar que Colombia necesita diseñar prontamente una estrategia de seguridad nacional, frente a las posibles amenazas provenientes del ciberespacio por parte de nuestro país vecino Venezuela.

Las amenazas informáticas crecen 15 por ciento cada año y la infraestructura colombiana no está bien preparada para afrontarlas. Según un estudio de la firma de seguridad informática Symantec, Colombia es el cuarto país más afectado en Latinoamérica por el fenómeno del secuestro de computadores para ser usados en ataques informáticos.

En el actual entorno de tensiones existentes con nuestros países vecino, Venezuela potencialmente puede llegar a acceder al conocimiento y tecnología necesaria para poder bloquear el espectro del ciberespacio de Colombia, gracias a sus alianzas con países como Cuba, Rusia y China.

A nivel mundial los líderes en el uso de las tecnologías de la información son Estados Unidos, China y Rusia. Actualmente Colombia aplica con los Estados Unidos una práctica diplomática denomina "*Respice Polum (mirar al polo)*"[60]. Gracias a esta política, Colombia podría aprovechar esta oportunidad para extraer el mayor conocimiento del ciberespacio y a su vez establecer alianzas fuertes para su defensa.

Las nuevas amenazas de carácter global y asimétrico provenientes del ciberespacio constituyen un nuevo riesgo de seguridad para las naciones de la aldea global.

Actualmente vivimos en la era digital, donde cada una de las naciones comienza a tener más conciencia que la nueva riqueza y poder es la información y que sólo aquellos países que sean capaces de administrarla y asegurarla correctamente podrán llegar a tener la ventaja estratégica en la lucha con otras naciones y la conquista de sus mercados.

---

[60] CARVAJAL, Leonardo, *"Tres años del gobierno Uribe (2002-2005): Un análisis con base en conceptos dicotómicos de política exterior"*, en OASIS, N.11, Bogotá: Centro de Investigaciones y Proyectos Especiales (CIPE) de la Universidad Externado de Colombia, 2005-2006. Pág. 136.

Colombia debe generar pronto un proceso de contención frente a las posibles aspiraciones de expansión territorial (ciberespacio) de Venezuela y sus aliados, porque de lo contrario podrían verse afectados sus intereses nacionales.

1. LA INFORMACION, UN ACTIVO ESTRATEGICO

"La excelencia esta en aquellos que someten al enemigo sin entrar en combate"[61].
Sun Tzu

Las naciones han comenzado a valorar la información digital como uno de los activos más valiosos, y ha depender cada vez más de los sistemas de información que la administran.

A principios de los 90s el profesor James Appleberry señaló que el conocimiento crece cada vez más rápido: "Todo el conocimiento humano alcanzado en tiempo de cristo se duplico hacia 1750; volvió a duplicarse, esta vez en mucho menos tiempo, hacia 1900; nuevamente se duplicó en 1950".

En la actualidad, el conocimiento humano, medido en función de un complejo conjunto de parámetros, se está duplicando cada 5 años y, para el año 2020, se prevé que lo hará cada 73 días"[62]. Esta afirmación sirve para preocuparnos cada vez de cómo Colombia debe prepararse cada vez mas para la avalancha de información que vendrá a futuro gracias a su presencia en el ciberespacio.

Las amenazas provenientes del ciberespacio se pueden clasificar como ciber crímenes, ciber terrorismo y ciber guerra. El peligro de los ciber ataques consiste en que el atacante desde cualquier lugar del planeta puede causar daños considerables con un mínimo de recursos invertidos, sin causar bajas humanas. Los ciber terrorista aplican la estrategia planteada por Sun Tzu, cuando recomendaba tratar de derrotar al enemigo sin entablar combate.

---

[61] SUN TZU. *El arte de la guerra*. Traducido por Samuel B. Griffith. Oxford University Press, New York, 1963.
[62] APPLEBERRY, James. *National and local forces at work Challenging times for creative people*, 1998.

Gracias a los avances tecnológicos y los avances en el campo militar, se ha podido acuñar un nuevo concepto dentro del marco de las guerras de cuarta generación, denominado guerra electrónica. Esta consiste en la actividad militar que utiliza la tecnología electrónica con el fin de explotar, contener o negar el uso de todos los espectros electromagnéticos incluyendo los elementos del Ciberespacio por parte del adversario y a la vez conservar la utilización de dicho campo para el beneficio propio.

2. EL CASO DE ESTONIA – PRIMERA GUERRA ELECTRONICA DEL SIGLO XXI

Los eventos de abril del 2007 en Estonia son un buen referente para lo que se ha declarado la primera guerra electrónica del siglo XXI.

Estonia es una ex republica soviética desde hace 16 años, ubicada en al mar báltico, con una población de 1.3 millones de personas. Siendo un país pequeño es el país mas interconectado de Europa, con una población altamente dependiente de los sistemas de comunicaciones e Internet para sus labores diarias.

El evento que desencadeno el ataque cibernético fue cuando las autoridades de Estonia decidieron mover una estatua de bronce de un soldado soviético de la II guerra mundial.

La estrategia aplicada en el ataque fue la de negación del servicio, que consiste en que simultáneamente cientos de miles de computadores accedan a los sitios Web objetivo para así mantenerlo ocupado y no permitir de esta forma atender a los usuarios que si desean hacer operaciones legítimas.

Los sitios Web atacados pertenecían al primer ministro, el parlamento, agencias gubernamentales, periódicos y el banco más grande de Estonia. Al finalizar las 3 semanas del ataque, las autoridades descubrieron que un oficial de la administración del presidente

Putin de Rusia estaba involucrado. Estonia confrontó a Rusia, la cuál oficialmente niega hasta el día de hoy haber liderado estos ataques.

Este ataque demostró, como es posible enfrentarse electrónicamente contra un país usando como base de lanzamiento de los ataques múltiples países al mismo tiempo. Sin que estos países necesariamente tengan conocimiento o estén de acuerdo con prestar sus conexiones a Internet al servicio de los atacantes.

El Ministro de Defensa de Estonia reconoció que habían desarrollado estrategias de combate contra ataques navales, bombardeos, tanques, pero contra un ataque digital nunca había sido previsto. Estonia tratando de neutralizar el ataque, solicitó apoyo internacional a sus aliados de la OTAN sin lograr resultados satisfactorios. Producto de las lecciones aprendidas la OTAN en Mayo del 2008 creo el centro de defensa del ciberespacio en Estonia[63].

Durante el período del ataque los ciber terroristas aplicaron como un instrumento de su poder, la negación a los ciudadanos a acceder a servicios estratégicos como la banca y las telecomunicaciones.

Rusia aplicó la estrategia de interferencia a Estonia tratando de generar un efecto favorable a su imagen, Putin negó cualquier implicación en el hecho aplicando uno de los principios de la interferencia denominado la "negación creíble".

3. UNA APLICACION DE LOS FUNDAMENTOS ESTRATEGICOS

En el ámbito del ciberespacio la teoría de Clausewitz que indica que las guerras son del dominio exclusivo del estado y se librarán solo entre estados, ha comenzado a ser

[63] *NATO launches cyber defence centre in Estonia*, acceso en http://en.kioskea.net/actualites/nato-launches-cyber-defence-centre-in-estonia-10374-actualite.php3 . Última consulta Octubre 11 2008.

reevaluado. Porque el ciber terrorismo ha demostrado que pueden ser emprendido por cualquier persona en cualquier lugar con un conocimiento cada vez más básico del Internet.

El uso de la tecnología en el marco de las guerras de cuarta generación se basa en la premisa, que al menos que se requiera, ya no existen razones para destruir al adversario, al contrario resulta de mayor utilidad su sometimiento público.

Retomando a Walzer en el capítulo de Amstutz dedicado a "La ética de la fuerza"[64], dice "que no obstante los problemas morales de la guerra de guerrillas, la insurgencia puede ser un medio moralmente legítimo para luchar contra la opresión". Es de esta forma como la nueva amenaza de ciberterrorismo justifica su accionar en contra de los gobiernos e instituciones que van en contravía de sus lineamientos.

Amstutz analiza como solo el 23% de los conflictos que se presentaron posterior a la guerra fría fueron entre estados, lo cuál ayuda a demostrar que la tesis expresada por Clausewitz del choque frontal y la batalla decisiva va en desuso y que los nuevos conflictos de baja intensidad y las guerras asimétricas son definitivamente las nuevas formas de hacer la guerra.

En el Ciberespacio como el nuevo campo de batalla, se aplican los mismos principios de la guerra. Los sistemas de cómputo e Internet ya no son solo del domino militar gracias a su masificación, por lo que estas tecnologías están en manos de individuos con modos de pensar muy diversos frente a las naciones e instituciones que los representan.

Estos individuos o naciones al no estar conformes con el pensamiento o acciones de una nación, pueden fácilmente convertirse en ciber terroristas al tener su objetivo a un clic de distancia.

---

[64] AMSTUTZ, Mark R. *La ética de la fuerza*. Capítulo 5 de la ética internacional, Oxford, Rowman & Littlefield. 1999.Pág. 93.

En el nuevo campo de batalla del Ciberespacio son varias los fundamentos de la lógica estratégica, que se pueden aplicar como instrumentos de uso del poder la Negación y la Interferencia y del uso de la influencia el Poder Invisible (Soft Power)[65].

Cada uno de estos fundamentos estratégicos ayuda a justificar el porque una nación debe tener una estrategia de defensa contra las amenazas del ciberespacio.

En la era de la información surgió una nueva forma de ejercer influencia denominada el poder invisible (soft power), término introducido por Joseph Nye en 1990. Nye sostiene que Estados Unidos es el país que mejor puede liderar la revolución de la información y que gracias a ello será el más poderoso. La información brinda ventajas que ayudan a frenar las amenazas militares a un relativo bajo costo[66].

4. APLICACION AL CASO COLOMBIANO

Colombia no se ha hecho a un lado frente al proceso de globalización que a nivel mundial las naciones vienen adelantando, este proceso implica retos, amenazas y oportunidades que afrontar.

En el ciberespacio un bajo nivel de seguridad de la información reduce la competitividad de las Naciones. A nivel mundial se consideran como objetivos a vulnerar, los sistemas de misión crítica como las telecomunicaciones, redes eléctricas, gasoductos, oleoductos, bancos, transporte, acueductos, servicios gubernamentales y servicios de emergencia.

---

[65] NYE, Joseph S. Jr., y William A. OWENS, *America's Information Edge*, publicado en Foreign Affairs, Marzo/Abril 1996, Pág. 20. http://usinfo.state.gov/journals/itgic/0996/ijge/gjcom6.htm . Última consulta Noviembre 22 de 2008.

[66] Ibíd.

La infraestructura informática de Colombia, ha mostrado ser vulnerable cada vez que un virus a nivel mundial ataca. Gracias al nivel de penetración de Internet que cada día va en aumento, y el alto nivel de piratería estimado en 58% para el año 2007[67].

Un ejemplo reciente en Colombia fue el denominado virus "Medellín"[68], programado para activarse el 5 de septiembre inactivando los computadores infectados. Este virus demostró como las instituciones públicas en Colombia como la Policía, Fiscalía, alcaldías, Gobernación, ECOPETROL y hospitales son vulnerables a esta clase de ataques programados. Es interesante notar que el ataque se centró principalmente en el departamento de Santander, en los municipios de Barbosa y Barrancabermeja.

Según estadísticas a nivel mundial los ataques de Internet se generan en primer lugar desde Estados Unidos, China, Alemania, y en noveno lugar Brasil[69]. Colombia ante estos fenómenos ocupa el cuarto lugar en America Latina.

Actualmente para Colombia uno de los países que podría implicar algún grado de amenaza dado su incremento de poder militar sería Venezuela. El cuál puede representar una amenaza debido a la posible utilización del poder potencial que tienen Rusia, China y Cuba para el dominio del Ciberespacio. Esta amenaza se podría representar en el bloqueo, interrupción, sabotaje u obstrucción de los sistemas de información críticos de Colombia.

En cuanto a China, Rusia y Cuba no se considerarían una amenaza directa a nuestra seguridad, pero indirectamente podrían influenciar al ser proveedores de tecnología militar y de conocimiento de Venezuela.

---

[67] *Colombia, el país menos pirata de la región* . Diario El Tiempo. 2008. http://www.eltiempo.com/tecnologia/enter/actualidad_a/home/colombia-el-pais-menos-pirata-de-la-region_4178223-1. Última consulta Octubre 11 de 2008.

[68] *El 'Virus Medellín' causa estragos en los computadores de Santander* http://www.caracol.com.co/nota.aspx?id=666183 Última consulta Octubre 11 de 2008.

[69] *Symantec Global Internet Security. Threat Report Trends for July–December 07.* Volumen XII, 2008. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf . Última consulta Octubre 7 2008.

El paso 27 de enero de 2008, el presidente Hugo Chávez comenzó a hablar sobre el ALBA (Alternativa Bolivariana para las Américas) Militar diciendo lo siguiente: "Deberíamos trabajar (...) para conformar una estrategia de defensa conjunta e ir articulando nuestras Fuerzas Armadas, aéreas, el Ejército, la Marina, la Guardia Nacional, las fuerzas de cooperación, los cuerpos de inteligencia, porque el enemigo es el mismo: el imperio de los Estados Unidos"[70].

Venezuela para aumentar su capacidad de manejo del espectro electromagnético en el mes de noviembre de 2008, puso en orbita su satélite Simón Bolívar construido por China y orientado a ampliar la capacidad actual de las telecomunicaciones[71].

En al año de 1994, Cuba negocia un acuerdo con Rusia, para la construcción de la base de guerra electrónica de Bejucal. Construida a un costo de $800 millones de dólares.

Actualmente, esta Base es operada por el gobierno cubano, y por un acuerdo de 1999 personal militar de la Republica Popular China opera de manera conjunta con los ingenieros cubanos para el monitoreo de las comunicaciones de Estados Unidos.[72]

En el caso de China las autoridades consideran a la seguridad de la información como uno de los puntos clave de su plan para desarrollar su sector informático en el periodo 2006-2020, por lo tanto ya ha comenzado a aplicar medidas para garantizar la seguridad en Internet.

---

[70] *Chávez pide alianza militar contra EE.UU.*
http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7212000/7212793.stm Última consulta Octubre 11 de 2008.

[71] *Listo satélite venezolano Simón Bolívar que expandirá telecomunicaciones.*
http://www.rnv.gov.ve/noticias/index.php?act=ST&f=14&t=79301 Última consulta Octubre 11 de 2008.

[72] *Castro: a threat to the security of the united states.*
http://www.globalsecurity.org/wmd/library/news/cuba/oagmc020.htm. Última consulta Octubre 11 de 2008.

Un ejemplo es la batalla que actualmente se libra entre hackers de China y Estados Unidos, que consisten en atacar páginas Web de cada unos de los países y reivindicar la violación del sitio Internet. China ha comenzado a crear incentivos para su industria informática con el propósito de sustituir los productos importados de Estados Unidos por productos nacionales. Igualmente los militares chinos mantienen competiciones de penetración a sistemas informáticos para identificar y reclutar miembros talentosos para su ejército cibernético.

Rusia gracias a la guerra fría desarrolló sus sistemas de interferencia y bloqueo de comunicaciones convirtiéndolo en un líder en campo de la guerra electrónica. Como se citó anteriormente el caso de Estonia, donde Rusia probó lo catastrófico que podría llegar a ser un ataque preventivo sobre una nación altamente dependiente de las redes de comunicaciones.

Estados Unidos luego de los acontecimientos del 11 de Septiembre, procedió a identificar las posibles amenazas provenientes de las guerras de cuarta generación. Se identificaron amenazas como el ciberterrorismo y la ciber guerra, que entran en choque con la capacidad que mantiene Estados Unidos para seguir ejerciendo su Poder Invisible.

Es así como Estados Unidos como potencia líder en el uso de las tecnologías de la información, público a comienzos del 2003 su estrategia nacional para Asegurar el Ciberespacio[73]. Esta estrategia se diseño ante la necesidad de proteger los sistemas de información interconectados en red y que se caracterizan por ser vitales para la sociedad.

Estados unidos plantea como objetivos estratégicos prevenir los ciber ataques contra su infraestructura crítica, reducir la vulnerabilidad nacional a los ciber ataques y reducir el tiempo recuperación y daños en el caso que ocurran[74]. Se contempla que en tiempos de paz

---

[73] *Estrategia Nacional para Asegurar el Espacio Cibernético.* www.whitehouse.gov/pcipb. Última consulta Octubre 11 de 2008.
[74] Ibíd., Pág. 8.

se debe estar alerta en caso de espionaje y en tiempos de guerra los adversarios podrían tratar de intimidar a los políticos y al pueblo atacando la economía y negando acceso a infraestructuras estratégicas.

En el documento de Visión conjunta 2020[75], los Estados Unidos define que sus fuerzas militares deben ser capaces de realizar operaciones en todas las dimensiones posibles incluyendo el de la información.

Al revisar la valoración de potenciales que otros países tienen frente a Colombia en su capacidad de manejo del ciberespacio, se vislumbra una gran oportunidad de convertirse en un actor importante en la utilización y empleo del Ciberespacio mediante la adquisición y uso de tecnologías de última generación.

Para lo cuál deberá actualizar sus sistemas de comunicaciones e innovar altamente en el uso de las tecnologías de punta. Sin desconocer que Colombia es un líder en términos del uso del ciberespacio, gracias a las estrategias de masificación de Internet que el gobierno nacional viene adelantando con el programa denominado "Agenda de Conectividad".

Colombia al desarrollar su estrategia de seguridad del ciberespacio podría tener en cuenta las siguientes recomendaciones:

- Colombia a través del Ministerio de defensa y del Ministerio de comunicaciones debe lanzar prontamente su primer satélite para apoyo de los sistemas de comunicaciones y defensa nacional. Gracias a su posición privilegiada en la zona ecuatorial se deberá aprovechar esta ventaja para lograr este objetivo.
- Colombia al fortalecer sus sistemas de seguridad digital aplicaría la estrategia de negación a los sistemas estratégicos por parte de posibles atacantes.

---

[75] *Visión conjunta 2020: Las fuerzas armadas de los Estados Unidos preparándose para el futuro.* http://usacac.army.mil/cac/milreview/spanish/NovDec01/jointvision.PDF. Última consulta Octubre 11 de 2008

- Igualmente se aplicaría la contención para mantener a Venezuela a raya, y que de esta forma no trate de atacar electrónicamente. Al igual que en la guerra fría cada nación ve su información como el objetivo a atacar por parte de las otras naciones y generaran tensiones.
- Al ser Colombia un aliado estratégico de los Estados Unidos en America Latina se puede aprovechar esta oportunidad para recibir a manera de ayuda exterior, el conocimiento, experiencia y tecnología necesaria para aprender a mejorar y desarrollar nuestras prácticas de seguridad digital. Esto se fundamenta en la teoría del poder invisible sostiene que los amigos de Estados Unidos tenderán a ser fuertes, y los estados fuertes tenderán a ser amigables[76].
- Colombia al ser miembro de la OEA podrá tomar un papel de liderazgo frente a las posibles amenazas que surjan del uso de las nuevas tecnologías de la información. La OEA ha definido unas normas relacionadas con la seguridad informática, con el propósito de poder sancionar moralmente por parte de la comunidad internacional los ciber ataques que se produzcan a algunos de sus países miembros.
- A nivel del Comando General de las FFMM de Colombia se debería crear una unidad dedicada a la defensa del ciberespacio.
- Se debería de incluir al sector privado en las labores de seguridad del ciberespacio. Al igual que otras naciones la defensa del ciberespacio no debe ser solo de responsabilidad del sector público. Sectores como la industria en la seguridad de redes.
- Establecer acuerdos de cooperación internacional para la defensa del ciberespacio de Colombia con países líderes en el uso de las tecnologías informáticas, como Estados Unidos e Israel. Para los servicios de inteligencia colombianos esta es una gran oportunidad para generar sus propias técnicas de ciber defensa y fortalecer sus equipos técnicos y humanos para presentes y futuras amenazas.

---

[76] GOMPERT, David C., "*Right Makes Might: Freedom and Power in the Information Age*," capítulo 3 en Zalmay Khalilzad, John P. White, Andrew W. Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare*. Informe RAND MR-1016-AF, 1999, Pág. 45. http://www.rand.org/publications/MR/MR1016/MR1016.chap3.pdf. Última consulta Octubre 11 de 2008.

- Al igual que el mundo real se podrían efectuar ejercicios a manera de juegos de guerra, pero de carácter ético con las fuerzas de defensa digital de nuestros aliados para aprender a prevenir y solucionar posibles ataques.

CONCLUSIÓN

Establecer una posición de contención como estrategia defensiva ante los posibles procesos expansionistas de las naciones vecinas de Colombia, contribuirá a disuadirlas de su voluntad de atacar los intereses nacionales vía el Ciberespacio.

Las guerras informáticas hoy día hacen parte de los conflictos armados que se encuentra en pleno desarrollo. Las investigaciones tecnológicas actuales en el sector de la Seguridad y la Defensa, se orientan a transformar tecnologías de informática en nuevas capacidades bélicas.

Diseñar una buena política de seguridad nacional del ciberespacio servirá de base para el planeamiento y desarrollo de operaciones de información en época de paz y de tensiones.

Falta suficiente camino por recorrer, para lograr un buen clima de seguridad informático en Colombia. Pero gracias a toda la cooperación internacional que se pueda establecer. Los niveles de riesgos serán minimizados y las amenazas de carácter asimétrico podrán ser neutralizadas más fácilmente.

CAPÍTULO IV

EL CIBERESPACIO COMO NUEVO ESCENARIO GEOPOLITICO: RETOS Y RECOMENDACIONES PARA COLOMBIA.

INTRODUCCIÓN

Las naciones históricamente han visto los diferentes espacios geográficos (tierra, mar, aire y espacio exterior) como las dimensiones sobre los cuáles la geopolítica puede efectuar sus análisis. Pero la era de la información ofrece una nueva dimensión de análisis geopolítico conocido como el "Ciberespacio"[77].

Entendiéndose por ciberespacio como la representación visual para el sistema humano de los datos extraídos de cada computador, conectados en un modelo de red de información computarizada y en el cuál los usuarios pueden compartir su información.

Los precursores de la geopolítica como Mackinder tenían en cuenta para sus consideraciones geopolíticas el terreno. Mackinder planteó la teoría del poder terrestre y los riesgos para el Reino Unido que dependía del poder marítimo. Definió la zona de Eurasia como el "HearthLand", y expresó lo siguiente "Quien domina la Europa Oriental controla el Heartland; quien domina el Heartland controla la Isla Mundial y quien domina la Isla Mundial, domina el mundo".

De igual forma el almirante Mahan expresó como el poder marítimo podía ayudar a los intereses de una nación a ser potencia, basado en la tesis que para llegar a ser poderosa se necesitaba dominar la industria, la cuál a su vez consumiría materias primas que deberían obtenerse de zonas donde los productos terminados serían comerciados[78].

---

[77] GIBSON, William. *Neuromancer*. Ace Books, 1984

[78] ROSALES, Gustavo. "*Geopolítica y geoestrategia liderazgo y poder · Ensayos ·*". Universidad Militar Nueva Granada, 2005. Pág. 34.

Con la aparición de la aviación, surgió un nuevo a espacio a ser dominado y surgió la teoría del poder aéreo expresado por Julio Douhet, quién tenía como premisa de su teoría la frase 'desde lo alto se ve bien y se hace blanco fácilmente'.

Posteriormente surge una nueva dimensión por fuera del globo terrestre y es el espacio exterior, Alvin Toffler en su libro "Las guerras del futuro" retoma el pensamiento de Mackinder e indica que los estados que dominen el espacio exterior dominaran el planeta Tierra.

Al revisar los cambios a nivel mundial que ha vivido el mundo a lo largo de los últimos dos siglos, se puede ver como la tecnología y la geopolítica son cambiantes, se adaptan y reflejan el dinamismo de la sociedad en su momento.

Este capítulo pretende demostrar que Colombia necesita prepararse para los retos que ofrece la nueva dimensión del Ciberespacio al servicio de la geopolítica, y como se puede convierte en un factor decisivo en el ejercicio de la soberanía y el poder nacional.

Se trata de estimular el pensamiento acerca de nuevos factores que pueden influir en la seguridad global y geopolítica, y de esta forma lograr recomendar posibles cursos de acción en el presente que ayuden a garantizar el futuro de Colombia en el escenario geopolítico de un mundo globalizado e interconectado.

La geopolítica cada día tiene más auge debido a la influencia de las tecnologías de la información (TIC) en las relaciones internacionales. Los espacios físicos gracias a la era de la información, se perciben cada vez menos como barreras para el conocimiento y el comercio. Anteriormente los sucesos que se daban en estados ubicados en zonas geográficamente apartadas de nuestro país, no influían necesariamente en las decisiones de otros estados.

Pero hoy día gracias a las redes de comunicaciones que recorren el mundo y lo interconectan, se ha generado un nivel de interdependencia cada vez mayor entre los estados.

Probablemente los países en el siglo XXI se enfocarán más en hacer parte de los procesos de globalización, que en disputar los espacios geográficos. Se prevé entonces, que las guerras de cuarta y quinta generación estarán a la orden del día.

Colombia gracias a su posición geoestratégica privilegiada a nivel latinoamericano y como un país deseoso de hacer parte de los procesos de integración comerciales, no ha sido ajeno al proceso de globalización.

La tecnología ha contribuido altamente al proceso de interacción entre los estados e igualmente ha permitido darle la categoría de nuevo espacio geopolítico al ciberespacio, gracias al flujo de información que permite las relaciones humanas

La información actualmente tiene varias características, una de ellas es que es tratada como un bien valioso para el que la posee y el que la desea[79]. El período de tiempo para que una persona obtenga la información gracias a las TIC es casi inmediato. Y la tercera característica es, que cada día que pasa es menos costosa, tendiendo a ser casi gratuita.

En el siglo XXI, cada día es más evidente la necesidad de información y conocimiento que los seres humanos necesitan consumir en su vida diaria. Se ve una gran oportunidad de desarrollar políticas de presencia del estado colombiano en el ciberespacio aprovechando estrategias de Soft Power ("Poder Blando") o atracción y preparándose para aplicar estrategias de coerción en caso de ser necesario.

---

[79] FEAL, Javier. *El poder mediático*, en Boletín No.283, CESEDEN – Ministerio de Defensa de España. 2004, Pág. 92.

1. UNA NUEVA DIMENSION DE LA GEOPOLITICA: "EL CIBERESPACIO"

Se puede partir del concepto de espacio vital dado por Friedrich Ratzel que indica que el Estado se comporta como un organismo vivo y como tal necesita espacio para crecer y moverse. Este mismo concepto se puede aplicar en la forma como un Estado puede crecer y moverse en el ciberespacio, gracias a que en esta nueva dimensión que no tiene fronteras más que las de la imaginación.

Las nuevas tecnologías han producido un cambio en la noción de tiempo y espacio, a causa de la forma como en el denominado tiempo real los acontecimientos de una nación se difunden al mundo de manera casi inmediata.

Anteriormente la geografía actuaba como contenedor natural de las noticias y por lo tanto la concepción del tiempo era diferente, ya que los acontecimientos políticos o militares no afectaban de manera tan directa como lo hacen hoy día, gracias a un mundo interdependiente en si mismo.

Uno de los autores que tiene en cuanta la influencia del ciberespacio en la geopolítica, es el autor alemán Karl Schlögel en su libro "En el Espacio Leemos el Tiempo. Sobre Historia de la Civilización y Geopolítica". Este filósofo analiza como los espacios sociales en el ciberespacio interactúan y se convierten en espacios virtuales y conforman un nuevo espacio denominado "Ciberia"[80].

El autor propone que la geopolítica no necesariamente tiene que estar ligada con los espacios geográficos, sino con el dominio del espacio virtual[81]. De esta forma propone comenzar a pensar en nuevas dimensiones y así dar paso a una nuevo pensamiento

---

[80] SCHLÖGEL, Karl. *En el Espacio Leemos el Tiempo. Sobre Historia de la Civilización y Geopolítica.* Traducido por José Luis Arántegui. Publicado por Siruela, 2007. Pág. 75

[81] Ibíd., Pág. 75.

geopolítico mas amplio. "Ciberia" es ese nuevo espacio donde aparece el "Infopoder"[82], gracias a que los flujo de información son la riqueza que hace a cada uno de los actores en la era de la información mas o menos poderos ante los otros.

Surge entonces el modelo de red, que descentraliza el concepto del poder atado a un sitio geográfico. De esta forma lo hace independiente del espacio geográfico.

Un ejemplo de ello se puede ver en las corporaciones multinacionales que operan bajo el concepto de redes, entrelazando sus nodos u oficinas con presencia a nivel mundial.

De esta forma el proceso de globalización se ha ido produciendo y cada vez más se pierde la noción que implica que una empresa con carácter multinacional pertenezca a un Estado determinado.

Al revisar los mapas de flujo de datos de Internet[83] se ve claro la frase que Schlögel cita "La digitalización ha dado paso a una nueva especialidad. El tránsito de geo-grafía a info-grafía parece haberse consumado"[84].

Revisando el mapa global de Internet se visualiza como la autopista de la información tiene mayor ancho de banda y apunta a interconectar a Estados Unidos principalmente con Asia, Pacífico, Europa y en mucho menor grado a Latinoamérica, Caribe y Africa.

Las naciones que mas enlazadas estén en la red tendrán un menor grado de desigualdad, y las menos conectadas al ciberespacio estarán en mayor grado de desigualdad frente a las otras naciones. Lo anterior ratifica mas la tesis que Colombia al no tener actualmente un

---

[82] GUTIÉRREZ, Víctor Manuel. *Espacio y Geopolítica*. http://mapppcolsan.blogspot.com/2008/06/espacio-y-poltica.html, Última consulta Febrero 22 de 2009.
[83] *Global Internet Map*, www.telegeography.com/products/map_internet/wallpaper/InternetMap09_wall2.jpg, Última consulta Febrero 22 de 2009.
[84] SCHLÖGEL, Karl. Op. Cit. Pag. 78

papel importante en el uso del ciberespacio, puede verse como una oportunidad para preparar a nuestra Nación para su correcto uso y aprovechamiento.

Dentro del mundo de Ciberia se conforma una realidad virtual donde las personas mas capacitadas para navegar en el se denominan "digerati"[85]. Se conformarán "naciones digitales" que no reflejaran necesariamente los Estados con territorio, sino que tendrán objetivos o intereses comunes en el ciberespacio y estarán unidos por su información.

Esto hace parte de la brecha digital que los estados deben disminuir. Los miembros hoy día que pertenecen a esta comunidad no necesariamente son los miembros más representativos de cada país, sino los mejor conectados al ciberespacio.

Así mismo, surgirán los "inforebeldes" que aprovecharán el ciberespacio como su campo de acciones. Implicando que los actuales y futuros enemigos probablemente no sean fáciles de ubicar en el espacio físico. El fenómeno de las migraciones asociadas al fenómeno de la globalización, es un buen ejemplo de cómo los ciudadanos buscan un mejor bienestar en países económicamente mejor y a su vez mejor informados e interconectados con el mundo.

A su vez la no pertenencia de las personas migrantes a un Estado territorial, puede generar conflictos internos o inestabilidades regionales a causa de los procesos de globalización.[86]

Ratzel previó lo que podría se el fenómeno de la globalización: "El mundo se ha empequeñecido tanto, que solo hay campo en el para una sola nación". Hemos visto que es un proceso de expansión a nivel mundial y de proyección de los estados con consecuencias étnicas, culturales, económicas, sociales y políticas. En la actualidad la globalización involucra a todo el mundo y se convierte en uno de los elementos representativos del mundo postmoderno.

---

[85] Ibíd., Pág. 79.
[86] Ibíd, Pag 81.

Hoy día es muy fácil para una compañía comenzar a globalizarse con solo publicar en Internet su sitio con capacidades de comercio electrónico y gracias a los buscadores como Google y los traductores de páginas las barreras del idioma son franqueadas.

Es bien sabido que una de las herramientas disponibles al servicio de la geopolítica son las relaciones exteriores, pero en el caso de ciberespacio se puede denominar "*Diplomacia en la Red*"[87] término acuñado por Zbigniew Brzezinski.

Este consejero presidencial durante el gobierno Carter vislumbro la integración entre las telecomunicaciones y la informática. El argumento que el proponia era que Estados Unidos gracias a su gran capacidad para dominar las redes mundiales de información podría difundir sus valores y de esta forma atraer e influir en otras naciones del mundo.

Años más tarde Joseph S. Nye como consejero de la administración Clinton retomaría el anterior concepto con denominándolo "Soft Power".

"El saber, más que nunca, es poder. Estados Unidos es el único país que está en condiciones de llevar a cabo por sí sólo la revolución de la información (...) Fuerza multiplicadora de la diplomacia estadounidense, el eje de las tecnologías de la información fundamenta el soft power, la seducción ejercida por la democracia estadounidense y los mercados libres"[88] .

Es así, como la información se considera el nuevo poder. Que fluye a través de la redes de telecomunicaciones, y alimenta de manera continua el ciberespacio. La información cada vez llega más pura desde la fuente hasta los consumidores. Un ejemplo de ello son los videos de las ejecuciones de AlQaeda, que sin pasar por ninguna censura llegan directo a los millones de usuarios de la Red.

---

[87] BRZEZINSKI, Zbigniew. *Between Two Ages*, Nueva York, Viking Press, 1969.
[88] NYE, Joseph S. y William A. OWENS, *America's Information Edge*, Publicado en Foreign Affairs, vol. 75, N° 2. 1996.

Este tipo de estrategias podríamos denominarlas el "Efecto Internet" a semejanza del denominado "Efecto CNN". Estamos presenciando un mundo cada vez mas sin intermediadores, a un mundo sin fronteras donde las personas pueden acceder directamente a los proveedores de bienes o servicios en segundos gracias a Internet.

El soft power, se puede emplear para influir en nuestros aliados y oponentes para hacerlos desear lo que posee nuestra nación, o aceptar formas de comportamientos de nuestra sociedad ante los ojos de otras naciones. Igual el poder blando ("Soft Power") opera de manera contraria a la estrategia de la coerción que obliga al adversario a hacer algo en contra de su voluntad.

La anterior estrategia empleada principalmente por los Estados Unidos, ha sido empleada de manera similar por otras potencias como Gran Bretaña, Alemania, Francia, Rusia, China, Brasil e India a nivel global.

2. CASOS DEL EMPLEO DEL CIBERESPACIO, DESDE UN ANALISIS GEOPOLITICO.

Se revisarán algunos casos que pueden ejemplificar el uso del Ciberespacio por parte de algunas organizaciones terroristas, de ciudadanos de bien que quieren enviar un mensaje como nación a un grupo armado y como un Estado monitorea a nivel mundial:

2.1. Caso de Al Qaeda y la Yihad Islámica (La e-Yihad y e-Qaeda):

Los grupos terroristas usan Internet de las siguientes formas[89]: Guerras sicológicas, publicidad y propaganda, minería de datos, recolección de fondos, reclutamiento y movilización, trabajo en red, compartir información y planeación-coordinación.

---

[89] WEIMANN, Gabriel. *www.terror.net How Modern terrorism uses the Internet.* publicado en United States Institute of Peace – Special Report. http://www.usip.org/pubs/specialreports/sr116.pdf. Último acceso Febrero 22 de 2008.

Aplicando las anteriores formas los nuevos grupos terroristas han identificado un medio de uso libre, masificado y en constante crecimiento para fomentar sus ideas, financiar su accionar, y mantener a sus miembros informados y conectados, adicionalmente atraer nuevos miembros y capacitarlos de una forma poco costosa y accesible desde todo el mundo.[90]

Para el actual caso vamos a revisar la organización terrorista AlQaeda, y digo organización porque se comporta como tal al tener una red financiera a través del mundo, con esquemas descentralizados que invierten tanto en negocios lícitos como ilícitos.

Ellos han adoptado el esquema de trabajo en red, donde cada nodo de la red se financia por si solo y no necesariamente depende la casa matriz para la obtención de recursos. Según cálculos del FBI los costos asociados para la realización de los atentados del 11 de septiembre de 2001 (11-S) fueron 500.000 de dólares[91], en el caso del 11-M en Madrid, se calcula que unos 105.000 de dólares[92], y para el del 7 de julio de 2005 (7-J) en Inglaterra se necesitaron unas 8.000 libras esterlinas[93].

Al revisar las cifras de acceso a Internet a nivel mundial se encuentra que los países musulmanes son los que más bajo nivel de penetración de Internet presentan, al igual que el manejo del idioma inglés. Pero Al Qaeda ha sabido explotar el espacio virtual de sus enemigos y lo ha usado en su contra. La gran mayoría de sitios Web orientados a promover la Yihad están situados en Estados Unidos y Europa.

---

[90] FLORES, María Lourdes. *Internet como herramienta del integrismo Yihadista.* Publicado en el Boletín No.303, CESEDEN – Ministerio de Defensa de España. 2004, Pág. 22.

[91] KEPEL, G., *La yihad. Expansión y declive del islamismo.* Barcelona, Ediciones Península, 2000.

[92] *Auto de levantamiento parcial del sumario,* Documentos 11-M Madrid. http://www.elmundo.es/documentos/2004/03/espana/atentados11m/documentos.html. Última consulta Febrero 22 de 2009.

[93] *Intelligence and Security Comittee (2006), Report into the London Terrorist Attacks on 7 July 2005.*, http://www.official-documents.gov.uk/document/cm67/6785/6785.pdf. Última consulta Febrero 22 de 2008.

Al momento de suceder los atentados del 11-S, Osama Ben Laden no era conocido por solo una parte del mundo, pero el punto mas alto a nivel mediático fue cuando aprovechando las cadenas de televisión reivindicó los atentados de NY.

El paso siguiente fue cuando Al Zarkawui comenzó a aprovechar el Ciberespacio como medio de transmisión de sus operaciones y medio de negociación con Osama Ben Laden para unificar esfuerzos. Al Zarkawui se convirtió en una estrella del Internet y abrió el camino para los terroristas en línea"[94] o "Inforebeldes, al publicar los videos de las decapitaciones sin intermediarios, ni censuras.

La causa de la Yihad necesita mártires dispuestos a dar sus vidas por la causa, y de forma similar como se hace con el comercio electrónico se deben publicar los contenidos que los clientes quieren y proceder a registrarlos en las bases de datos para luego fidelizarlos y conducirlos a comprar sus ideas.

Haciendo uso de Internet no solo se atraen creyentes en la causa sino contribuyentes que la financien. AlQaeda ha logrado hacer uso efectivo de Internet como herramienta de reclutamiento ya que parte de sus miembros cuentan con edades promedios entre los 20 y 30 años que saben hacer uso de las TIC, debido a que han migrado a países donde han aprendido como aprovecharlas en su beneficio.

Luego de reclutar a los simpatizantes hay que formarlos, enseñarles tácticas de cómo operar y como encriptar la información que envían para que las herramientas de detección de terrorismo no los rastreen.
Los estrategas de AlQaeda han entendido y empleado el concepto denominado "Guerra de Redes" (*"NetWar"*), termino empleado dentro de las guerras de cuarta generación.

---

[94] GLASSER, S. y S. Coll, *The Web as Weapon.* publicado en The Washington Post. 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html. Última consulta Febrero 22 de 2009.

Han diseñado un modelo que divide la estructura de la célula en grupos cada uno con funciones complementarias así[95]: la alta comandancia, el grupo de liderazgo, el grupo para reunir información, el grupo dedicado a aprovisionamiento y el de ejecución.

De esta forma el nuevo movimiento yihadista (e-yihad) aprovecha el Ciberespacio para atraer nuevos creyentes y fidelizarlos, con el objetivo de tratar de cambiar el Status Quo mediante el uso del terrorismo en el espacio físico de la geopolítica y todo esto gracias a la libertad de expresión que se puede ejercer en "Ciberia".

2.2. Las redes sociales virtuales al servicio de la expresión de los ciudadanos: Caso del 4F – Movilización Mundial en Colombia contra las FARC:

Los cibernautas colombianos han hecho que Colombia se posicione entre los 10 países con mayor número de usuarios de las redes sociales virtuales y en particular de Facebook.com, a la cuál actualmente están afiliadas cerca de 3'709.183 colombianos generando una revolución en las relaciones interpersonales.

En diciembre de 2007 inteligencia del ejército interceptó pruebas de supervivencia que mostraban en pésimo estado de salud a los secuestrados políticos de las FARC, como Ingrid Betancourt, 3 contratistas del gobierno de los Estados Unidos y policías y miembros del ejército.

Estas pruebas tocaron la fibra de los colombianos y generó la iniciativa de un grupo de colombianos denominado "Colombia soy yo", los cuales de manera ingeniosa lograron aprovechar el concepto de redes sociales virtuales en el ciberespacio a través de sitio www.facebook.com.

Procedieron a crear un grupo de convocatoria para una marcha en contra de las FARC para el 4 de febrero de 2008, concluyendo con la afiliación de más de 250.000 mil miembros de la red social Facebook. Este fenómeno virtual de manera conjunta con los grandes medios

[95] FLORES, María Lourdes. Op. Cit. Pág. 52.

de comunicación y del gobierno, logró convocar cerca de 10 millones de colombianos con el ánimo de protestar en contra la organización narcoterrorista FARC.

Esta fue una contundente muestra simbólica y pacífica del inconformismo de una Nación en contra de de la guerrilla de las FARC. Lograr esta identificación por parte de los ciudadanos colombianos de manera casi unánime, fue novedosa en el país. Al alcanzar que sin distingo de condición de riqueza o pobreza, educación, religión, color de piel se unieran para marchar en contra de un enemigo común.

Como efecto de la marcha se sentó un precedente para los futuros mandatarios del país, y es que a las FARC se deben combatir, derrotar y obligar a negociar. Políticamente las FARC anunciaron rápidamente la liberación de Clara Rojas y Consuelo González de Perdomo por razones de salud, tratando de minimizar los efectos de la contundente marcha en su contra.

Este proceso de convocatoria virtual para realizar un evento en el mundo real, es un ejemplo de cómo el gobierno colombiano puede aprovechar el Ciberespacio para tratar de influir políticamente sobre los actores armados del país.

2.3 Proyecto ECHELON y CARNIVORE para inteligencia de señales:

Los gobiernos de Australia, Canadá, Nueva Zelandia, Reino unido y los Estados Unidos previendo el incremento del flujo de señales que envían información utilizando las telecomunicaciones han formando un proyecto de monitoreo de comunicaciones llamado Echelon[96].

Este proyecto fue concebido para actuar de manera preventiva millones de comunicaciones telefónicas, fax y correos electrónicos, transmitidos vía satelital, redes de microondas y redes telefonía pública local y celular. El sistema en capacidad de interpretar el contenido

---

[96] ASSER, Martin. *Echelon: Big brother without a cause?*. BBC News. 2000. http://news.bbc.co.uk/2/hi/europe/820758.stm. Última consulta Febrero 22 de 2009.

de las comunicaciones y generar alertas a los operadores cuando se mencionen palabras claves relacionadas con terrorismo como AK47, Anfo, etc.

Este proyecto creado durante el período de la guerra fría aunque exitoso en su momento, tiene una debilidad y es que fue diseñado pensando en interceptar las comunicaciones vía satélite. Hoy día la mayoría de las comunicaciones se transmiten a través de fibra óptica por su bajo costo frente a las comunicaciones satelitales.

Al comienzo de Internet la mayoría del tráfico era enrutado a través de los Estados Unidos y Europa, pero a medida que se tendían la red interconectada de fibra óptica el flujo de datos entre usuarios de un mismo país no tenía que viajar hacia Estados Unidos para regresar a su país de origen.

A partir de este proyecto el FBI previendo la penetración de Internet a nivel mundial, creo el proyecto Carnivore durante la administración Clinton[97]. Este Ciberpolicía fue nombrado así porque persigue la "carne" dentro los mensajes de correo electrónico que envían los usuarios de Internet.

El FBI procede a instalar sus equipos de monitoreo directamente en las instalaciones de los proveedores de acceso a Internet, ya que la fibra óptica se interconecta en sus sedes centrales. Luego de los atentados del 11 de Septiembre del 2001, tomó aun mas respaldo el monitoreo de Internet debido a que el FBI demostró que la gran parte de la preparación de los atentados fue planeada usando correos electrónicos.

3. RETOS PARA COLOMBIA

Hoy día gracias a las tecnologías de información y comunicaciones (TIC) casi cualquier colombiano habla sobre la crisis económica a nivel mundial, habla sobre el TLC. Esta

[97] VENTURA, Holly E. *Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power.* Critical Criminology .2005. http://www.cas.sc.edu/socy/faculty/deflem/zgovernterror.html. Última consulta Febrero 22 de 2009.

nueva clase de colombiano en el siglo XXI, es cada vez más informado y preocupado por el acontecer geopolítico a nivel mundial a comparación de nuestras anteriores generaciones.

Las llamadas TIC son una manifestación de la sociedad postmodernista, que se ve influenciada por los flujos continuos de información. Colombia gracias a su posición geográfica no se ha aislado de este proceso de interconexión comunicacional con el mundo.

Las últimas encuestas de penetración de las tecnologías de telefonía móvil indican que hay casi 33 millones de teléfonos celulares activos en el país, y probablemente a finales del 2009 serán cerca de 40 millones de teléfonos móviles en las manos de los ciudadanos colombianos.

Este efecto muestra el porque Colombia es uno de lo países mas ávidos por conocimiento, de cada vez estar mas conectado con el mundo, por aprovechar las TIC para generar negocios. Es ahí donde se encuentran las grandes oportunidades y retos que Colombia debería aprovechar y solucionar, para convertirse en un país influyente en el ciberespacio. Llevando su cultura a otras latitudes, modernizar nuestras industrias e integrarlas a los procesos de globalización.

Aprovechar los procesos de interconexión con el mundo puede generar mayor confianza de la comunidad regional y mundial. Claro esta, que al ser cada día más dependientes de las nuevas tecnologías, se pueden generar vulnerabilidades. Para las cuáles se debe estar preparado como nación, para proteger y ejercer soberanía sobre su ciberespacio.

Colombia como Estado debe estar preparada para conquistar y tomar un papel de liderazgo, en esta nueva dimensión que se ofrece. Y de igual forma para defenderlo de sus posibles enemigos que deseen vulnerar sus intereses.

El gobierno debe diseñar una estrategia nacional para la defensa y seguridad del ciberespacio colombiano. Esta estrategia debe ir encaminada a defender a Colombia de

posibles ataques contra los intereses nacionales que se perpetren o planean aprovechando la red Internet.

Se debe promover la reforma de las leyes para crear una ley de seguridad nacional que contemple de manera preventiva y regulada el monitoreo de páginas Web soportadas en el territorio colombiano.

Igualmente fortalecer las capacidades de monitoreo preventivo de correos electrónicos por parte de las autoridades judiciales. Todo lo anterior sin llegar a vulnerar los derechos y libertades básicas de los ciudadanos, teniendo cuidado de no convertirse en un gobierno autoritario.

Las fuerzas armadas de Colombia deberían prepararse tecnológicamente, para el caso que organizaciones al margen de la ley u otros estados. Que remotamente inicien un ataque en contra de los sistemas vitales de nuestro país.

Se debe inscribir como parte de los intereses nacionales la presencia y protección del ciberespacio colombiano. En el documento Visión 2019 del Departamento Nacional de Planeación reconoce la importancia de avanzar hacia una sociedad mejor informada[98].

Colombia como estado reconoce por fin que la información es un derecho que ayuda a obtener más y mejor conocimiento. En el plan de desarrollo se trazan como metas lograr que el 100% de las entidades públicas hagan parte de una gran red gubernamental y lograr una penetración de Internet al 60% de la población.

Actualmente Colombia ocupa el puesto 80 en el índice de oportunidad digital (IOD), que mide el progreso en el cierre de la brecha digital de un País[99]. Delante de Colombia están

---

[98] *Avanzar hacia una sociedad mejor informada.* Departamento Nacional de Planeación. http://www.dnp.gov.co/PortalWeb/Portals/0/archivos/documentos/2019/Documentos/Documento%20SOCIEDAD%20MEJOR%20INFORMADA.pdf, última consulta febrero 23 de 2009.

[99] Ibíd. Pág. 9.

Chile, Argentina, México y Venezuela, y después de Colombia los otros países de Latinoamérica y del Caribe.

Para ayudar a reducir el analfabetismo informático se debe invertir en capacitación y crear las competencias necesarias para al menos poder navegar en Internet.

La principal competencia a desarrollar es la capacidad de dominar el idioma inglés. El 57.4% de los contenidos de disponibles en Internet se encuentra en idioma inglés y sólo el 4.3% en español[100].

Se deberá regular tanto el uso y la vigilancia del ciberespacio en Colombia, el uso por parte de los ciudadanos para declarar a Colombia como un estado libre del Ciberterrorismo. Y regular su correcta vigilancia por parte de los organismos competentes para tal propósito.

Se recomienda trabajar en conjunto con el sector privado, aplicando el concepto de responsabilidad social para los proveedores de los servicios de Internet y fomentar la educación sobre contraterrorismo.

Actualmente leyes de reciente vigencia en Colombia como la de Habeas Data y la ley que regula los delitos informáticos en Colombia, son un primer paso para la regulación del ciberespacio en nuestro país. Sin embargo, se recomienda crear artículos que se articulen dentro de la ley de seguridad y defensa nacional para dar herramientas legales al gobierno nacional para la defensa y monitoreo del ciberespacio.

Por último se recomienda impulsar aún mas la investigación y el desarrollo (I+D) tecnológico. Particularmente en las áreas de informática y telecomunicaciones.

Se puede apoyar en la creación de redes tecnológicas avanzadas en coordinación con la industria y las universidades.

---

[100] Ibíd. Pág. 17.

CONCLUSIÓN

La geopolítica y la tecnología son de carácter cambiante y cada día influencian de manera más profunda la forma de ver el mundo, por lo tanto afecta la forma como la geopolítica efectuará sus análisis a futuro.

La nueva dimensión del Ciberespacio junto con el Infopoder se expanden día a día, y Colombia no puede ser ajena a estos procesos. Más aún cuando los analistas prevén que las futuras guerras de quinta generación se darán entre organizaciones que operan en red, por lo cuál debemos estar preparados.

Colombia como estado debe prepararse desde ya, y aprender de las experiencias de otros países en cuanto a lo bueno y malo del uso del Ciberespacio como parte de sus intereses nacionales.

Los futuros gobiernos deben invertir aún más en educación, investigación y desarrollo y en el manejo básico del idioma inglés.

CAPÍTULO V

NECESIDAD DE UNA POLITICA DE CIBERDEFENSA EN COLOMBIA

"La victoria sonríe a aquéllos que anticipan los cambios en el carácter de la guerra, y no a aquéllos que esperan adaptarse después de que hayan ocurrido dichos cambios".
Giulio Douhet, "El comando del aire".

INTRODUCCIÓN

La política de defensa de Colombia como estado actualmente esta centrada en el conflicto interno y el narcotráfico, y al comenzar a hablar de postconflicto es un momento oportuno para preparar la nación para contrarrestar las nuevas amenazas terroristas que a nivel mundial pueden atentar contra el estilo de vida de la sociedad en la era de la información.

La tendencia hoy día en las telecomunicaciones es la convergencia de los sistemas de transmisión de radio, televisión, telefonía y datos a usar un medio de transporte común denominado Internet.

Esta convergencia de medios de comunicación ha facilitado el desarrollo de nuevos espacios de interacción como el comercio electrónico, el gobierno en línea, la telemedicina, la educación en línea, las operaciones militares en red, entre otros.

El ciberespacio[101] presenta a su vez nuevos retos sobre el territorio de los países, en las denominadas fronteras virtuales de Colombia, las cuáles deben ser fortalecidas y defendidas.

Conceptos como la "legítima defensa" del ciberespacio o los "ataques preventivos" se encuentran en las primeras etapas de su reglamentación por parte de las leyes internacionales.

---

[101] GIBSON, William. Op. Cit.

Una prueba de ello es el ciberataque a Estonia supuestamente por parte de Rusia. A partir de este ataque se establecieron convenios de ciberdefensa con la OTAN, creando el primer centro de para la ciberdefensa del tratado del atlántico norte en Estonia para estudiar este nuevo tipo de guerras[102].

Los posibles ataques del ciberterrorismo podrían estar encaminados al comercio electrónico, la banca electrónica, sistemas de información militares, sistemas energéticos, sistemas de tráfico aéreo y sistemas de acueductos

Algunos analistas dice que "Colombia siempre ha mirado hacia el Interior", y no es una excepción el caso del espacio virtual, históricamente Colombia no ha tenido una fuerte presencia e interés por los asuntos fronterizos. Se debe incentivar aún mas la conciencia de los colombianos por la defensa de este nuevo espacio.

Existe una ventaja en el ciberespacio y es que nuestros nuevos países de frontera no son solo los 5 actuales en el espacio terrestre, en este nuevo espacio cualquier país del mundo podría servir de base para lanzar un ataque o amenaza ciber-terrorista contra Colombia. Se podría pensar en una nueva forma de diplomacia y sería la ciber-diplomacia. Ya en el pasado se ha hablado de las "fronteras ideológicas"[103].

Autores como Alfred T. Mahan que desarrollo los conceptos del poder naval, presentó la tesis que en tiempos de paz es el momento más propicio para construir una armada.

Retomando este concepto, Colombia debe crear su fuerza para la Ciberdefensa desde ahora y no esperar a que se presenten eventos de seguridad que afecten al país.

---

[102] *NATO opens new centre of excellence on cyber defence.* http://www.nato.int/docu/update/2008/05-may/e0514a.html . última consulta junio 15 de 2009.

[103] ANGELONE, Juan Pablo. *Doctrina de la Seguridad Nacional y Terrorismo de Estado: Apuntes y Definiciones*. http://infoderechos.org/es/node/178. última consulta junio 15 de 2009.

Las nuevas amenazas terroristas han demostrado que pueden ser mutantes y adaptarse para operar con tácticas de cuarta generación, tanto en tierra, mar, aire y el ciberespacio.

Hoy día el 90% de los bienes que fluyen a través del mundo se transporta por el Mar, de igual forma el flujo de transacciones comerciales que se mueve a través del ciberespacio corresponde a un gran porcentaje. Mahan expresó la teoría del bloqueo naval al comercio de un país con el propósito de hacerlo colapsar económicamente, aplicando una estrategia de negación.

De manera similar las nuevas formas de terrorismo y de guerra han comprendido que para poner en jaque a un estado, se pueden emplear las tácticas de negación a los servicios electrónicos de información en el ciberespacio del país.

Hoy día se ve el fenómeno que la seguridad en Internet esta en manos de compañías privadas, y en contraparte existen los "Mercenarios de Internet". Dispuestos a combatir por quien este dispuesto a pagar el precio sus servicios, con tácticas de guerra de guerrillas y tenga la necesidad de atacar ciertos blancos, y a su vez no quiera ser descubierto.

La tendencia a nivel mundial, consiste en que la información de las personas o entidades sea almacenada en la "nube" de Internet, lo cuál hace que el ciberespacio se convierta en un nuevo espacio de interés a defender y preservar libre de amenazas para su seguridad.

Recientemente el departamento de defensa de los estados unidos restringió el acceso de los ciudadanos a los servicios de mensajería instantánea en Internet, desde países sancionados como Cuba, Irán, Corea del Norte, Sudan, y Siria[104]. Este tipo respuestas demuestran como el ciberespacio se convierte en una nueva expresión de la geopolítica.

---

[104] *Microsoft suspende el 'Messenger' en los países embargados por EEUU. Mayo de 2009.* http://www.elmundo.es/elmundo/2009/05/26/navegante/1243360629.html . última consulta junio 16 de 2009.

El propósito de este capítulo es el de plantear la necesidad de establecer una política de defensa del ciberespacio de Colombia por parte del gobierno nacional.

Para ello se revisarán las nociones, políticas y algunas de las expresiones de ciberdefensa de las naciones líderes en la era de la información. Se revisará el estado actual de Colombia frente a los retos que presenta la era de la información, y las acciones tomadas por el gobierno colombiano con respecto a la ciberseguridad.

Todo lo anterior con el propósito, de hacer énfasis en la importancia de ser preventivos y no reactivos ante esta nueva clase de potencial amenaza. Para ello, se presentarán una serie de recomendaciones y reflexiones sobre algunas de las posibles acciones a seguir para fortalecer los niveles de la ciberdefensa de la nación.

1. UN NUEVO ENFOQUE POLITICO PARA LA CIBERDEFENSA

En la era de las comunicaciones digitales, la unión de la información y el poder se han unido a través del denominado "poder blando" que definió Joseph Nye. Las capacidades tecnológicas para acceder y producir información, por parte de las naciones se han incrementado en forma exponencial. Pero no en la misma magnitud se ha incrementado, la capacidad de entender y usar en el aspecto político y de defensa de la información.

Esta nueva forma de geopolítica, basada en la era de la información se denomina la "noopolitik"[105].

La noopolitik es el equivalente a la realpolitik, pero en el mundo construido por la redes comunicaciones denominado "noosfera". El concepto de la noosfera fue reforzado por el visionario Pierre Teilhard de Chardin, para describir a la capa virtual en la cual vive el conocimiento y la inteligencia colectiva.

---

[105] ARQUILLA, John y David RONFELDT, *The Emergence of Noopolitik*. National Defense Research Institute-RAND, 1999. Pág. 2. http://www.rand.org/pubs/monograph_reports/MR1033/MR1033.sum.pdf . última consulta junio 15 de 2009.

La noosfera se conceptualiza como la capa siguiente a la Litosfera y la biosfera. La noopolitik se basa entonces en el aprovechamiento y uso de la información para influenciar o atraer a otras naciones o culturas, con nuestro estilo de vida y forma de actuar y pensar.

Es decir, el uso del poder blando como una herramienta estratégica en la era de la información.

Basado en la frase expresada por Clausewitz: "La guerra es la continuación de la política por otros medios"[106]. Así mismo, se podría decir de la noopolitik en la era de la información es la continuación de la política a través del nuevo medio del Ciberespacio.

Afirma Nye, que un poder blando desarrollado incrementará la competitividad de un Estado en la era de la información.[107] Gracias a que presentará ante los otros países, la capacidad de adaptarse a las nuevas expresiones de cultura y conocimiento. Y de ninguna manera es aislacionista, y que su agenda como estado no se limita solo al ámbito interno, sino al internacional.

La noopolitik está orientada a la primacía del soft power, las redes de aliados vitales para la seguridad vs. las alianzas condicionadas, la primacía de intereses compartidos vs. la primacía del interés nacional, la propensión a compartir información vs. la vigilancia de los flujos de información. [108]

Como parte de los fundamentos para las políticas de ciberdefensa de las naciones, se deben establecer alianzas o coaliciones internacionales, ya que el atacante se puede esconder detrás de la población civil y pasar desapercibido. El poder del los ataques en el ciberespacio, es similar a la estrategia planteada por Douhet. Este teórico del poder aéreo, defendía los bombardeos a la población civil. Con el ánimo que el pueblo dejara de apoyar a los gobiernos de su nación.

---

[106] CLAUSEWITZ, Karl von, *De la guerra*, Ed. La Esfera De Los Libros. 2005.
[107] NYE, Joseph S., *La paradoja del poder norteamericano*. Madrid, Taurus, 2003. Pág. 105.
[108] ARQUILLA, John y David RONFELDT. Op. Cit. Pág. 47.

2. EJEMPLOS DEL EMPLEO DE LA CIBERDEFENSA

Los estados cada vez mas se interrelacionan en un ambiente globalizado e interdependiente de otras naciones, altamente complejo y en un medio ambiente en continuo cambio. El Ciberespacio se puede ver como un nuevo campo de acción de la geopolítica, y por lo tanto se ve involucrado con el comercio, la economía, el gobierno y la seguridad nacional.[109]

Para los estados la denominada seguridad regional esta basada en el dominio de los espacios terrestres, marítimos, aéreos, pero en el ciberespacio se puede hablar de domino global[110]. El ejerció de los poderes tradicionales de las fuerzas armadas se ven limitados a las fronteras establecidas para los estados, pero en el ciberespacio se puede dar la ubiquidad y con alcance global y sin violaciones de la soberanía.

Algunos regimenes al verse abocados a participar en Internet, han implementado algún cierto nivel de control de las comunicaciones por parte del nivel gubernamental. Tal es caso de China, que dedica cerca de 30000 empleados a monitorear las actividades en Internet[111]. Otros países consideran que el acceso de sus ciudadanos al Ciberespacio puede considerarse una posible amenaza, [112]

Se puede llegar a pensar que las posibles vulnerabilidades que se presentan en el Ciberespacio son pocas. Gracias a que desde la formación de Arpanet, la red predecesora de Internet. Sus orígenes fueron desde el principio originados en organizaciones militares que

---

[109] *The national military strategy for cyberspace operations*, 2006. http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf. última consulta junio 15 de 2009

[110] HANSEL, Mischa. *Challenging Regional Power and Security: Conflicts in Space and Cyberspace*. 2009. http://www.dgap.org/midcom-serveattachmentguid-1de451acbc2880e451a11de80a70dfed144ae4dae4d/2009_dgapbericht-14_nfc-2008_www.pdf. última consulta junio 15 de 2009

[111] LEWIS, James A. *The Architecture of Control: Internet Surveillance in China*, http://www.csis.org/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf. última consulta junio 15 de 2009.

[112] *Reporters without Borders, The 15 Enemies of the Internet and other Countries to Watch*, http://www.rsf.org/print.php3?id_article=15613 . última consulta junio 15 de 2009

pensaban en la alta disponibilidad y defensa de la nación. Pero no se puede desconocer que no contaban con los denominados virus de las computadoras que desde sus orígenes han demostrado que pueden causar mucho daño a la información.

Uno de los aspectos claves de la ciberseguridad es garantizar la protección de infraestructura crítica como los sistemas financieros, servicios públicos y telecomunicaciones. Ya que cada vez es mayor la dependencia de redes de datos que garantizan su normal y correcto funcionamiento.

En el caso de Colombia, se puede pensar que es menos costoso contaminar el sistema de datos de trasmisión eléctrica de la nación con un virus de computador, que dinamitar torres eléctricas.

En la era industrial la fortaleza de un país se pensaba en función de sus industrias y de sus fuentes de recursos naturales, los cuáles podrían ser atacados y conquistados por las fuerzas armadas de una nación enemiga. Hoy día es innegable el hecho que vivimos en una sociedad que cada día se hace más dependiente de la capacidad de obtener la información en tiempo real.

En consecuencia, se deben aumentar las medidas de seguridad para prevenir las posibles pérdidas económicas producto de amenazas provenientes del Ciberespacio. Anteriormente el dominio de la fuerza principalmente se soportaba por los ejércitos al servicio de la nación, y de manera igual con sus estados contendientes.

De esta forma, es como se diseñaban las estrategias de defensa. Pensando en conflictos de primera, segunda, tercera y cuarta generación como los denomina Lind.

En la actualidad revisando las guerras de cuarta generación que se basan en conflictos asimétricos, donde el adversario parte de la base de ser poco identificable y de no cumplir

las reglas de la guerra tradicionales. Se puede observar como este modelo es aplicado y mejorado en los ciber-ataques y ciber-crímenes.

Para los atacantes no existen las restricciones de las fronteras geográficas, pueden actuar con pocos recursos económicos, pueden pasar desapercibidos en el mundo real, construyen su capacidad de conocimiento y doctrina del tema muy rápidamente a comparación de la formación de un ejército armado. Y de manera similar gracias al don de la ubicuidad que brinda Internet, pueden lanzar de manera simultánea ataques desde un millón de computadoras a sus adversarios al mismo tiempo.

Para un potencial atacante sus armas pueden ser los virus de computador que se encargan de descargar a manera de caballos de Troya, herramientas de software malicioso. Estos programas logran que la máquina infectaba a manera de zombie, actúe sin saberlo para los propósitos deseados del atacante.

Esta capacidad de formar redes de computadores por miles o millones, se denominan "Bot Nets" o "Bot Networks". Estas redes de computadores, se pueden alquilar a manera de ejércitos mercenarios del ciberespacio. Se estima que el alquiler de una de estas redes puede costar entre 200 a 300 dólares la hora[113], lo cuál demuestra lo económico y relativamente fácil de acceder a las capacidades de lanzar ataques coordinados. Un ejemplo del uso de ataques basados en botnets, se presentó en 2007 contra Estonia.

Bajo estas perspectivas el nuevo centro de gravedad para las guerras cibernéticas son las redes de información.

---

[113] WILSON, Clay. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. http://www.ipmall.info/hosted_resources/crs/RL32114_080129.pdf . última consulta junio 15 de 2009

En el caso de Kosovo, conflicto de Israel y Palestina, entre Pakistán e India, Chechenia y Rusia[114], y recientemente Georgia y Rusia y Corea del Norte con Corea del Sur. Grupos de denominados hackers tratan de obtener información vital del enemigo o negarle acceso a recursos informáticos vitales. Esta es una demostración como los conflictos armados del mundo real, se trasladan al ciberespacio.

Días antes de iniciarse el conflicto de Rusia con Georgia[115], comenzó un ataque de negación de acceso a los visitantes a través de Internet de las páginas gubernamentales del gobierno de Georgia. Un año antes Rusia se había visto culpada por el ataque de un millón de computadores a las páginas Internet oficiales de Estonia.

En el caso de Estonia no pudo reaccionar a los supuestos ataques de Rusia en 2007. Pero producto de las lecciones aprendidas, Georgia aprendió que la maniobra y las alianzas eran claves para su ciberdefensa. Tan pronto comenzaron los ataques,[116] migró sus servicios de páginas Internet, a sitos de empresas privadas en Estados Unidos. Con el propósito de continuar con la operación de servicio, poder seguir comunicándose virtualmente con sus ciudadanos y poner en manos de terceros la defensa de la información gubernamental de Georgia.

Para algunos analistas esta clase de maniobra de llevar hacia territorio de Estados Unidos parte de los servicios informativos de una nación en conflicto, rompe con la ciber-neutralidad. Este se convertirá a partir de ahora un nuevo aspecto de investigación para los analistas de ciberguerras y para la aplicación de las leyes internacionales, cuando un país deja de ser neutral al prestar ayuda a una nación en ciber-conflicto.

---

[114] BILLO, Charles G. y Welton CHANG. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* . Pág. 14. http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf. última consulta junio 15 de 2009.

[115] *Guerra entre Rusia y Georgia pasó del terreno de batalla a portales de Internet.* http://www.portafolio.com.co/bienestar/cienciaytecnologia/2008-08-14/ARTICULO-WEB-NOTA_INTERIOR_PORTA-4445060.html . última consulta junio 15 de 2009

[116] *Russian hackers continue attacks on Georgian sites.* http://www.wjla.com/news/stories/0808/543487.html. 2008. última consulta junio 15 de 2009.

En el ciberespacio se puede presentar un dilema y es el como distinguir los objetivos militares, de la población no combatiente. Una mala interpretación de un evento de este tipo, podría desencadenar en un incidente internacional. Esto abre un buena línea de investigación y es la de cuáles serían las reglas de las guerras cibernéticas a aplicarse en los conflictos internacionales o de carácter asimétrico.

En la era de la información las nuevas formas de guerra, necesitan nuevas reglas que las ayuden a regularse.

Otro ejemplo reciente de conflictos llevados al ciberespacio es el de Corea del Norte y Corea del Sur. Se estima que el gobierno de corea del norte a entrenado una fuerza de 100 oficiales del ejercito dedicados a operaciones de ciberguerra[117].

No se debe olvidar que Estados Unidos es un aliado natural de Corea del Sur, y tiene cerca de 28500 hombres destacados como parte de una estrategia de disuasión contra algún tipo de acción bélica de corea del norte.

Es interesante ver como Kim Jong II actual líder de Corea del Norte, controla el acceso a Internet de sus ciudadanos. Pero a su vez promueve que quien no sepa usar un computador en el siglo XXI es un tonto[118]. Este líder ha identificado que puede explotar de su enemigo natural Corea del Sur, su alta dependencia de los servicios que presta Internet. De nuevo se puede observar como Estados unidos acaba de firmar un convenio de cooperación, para la defensa del ciberespacio de corea del sur.

---

[117] *Corea del Norte se infiltra en las redes informáticas del Ejército de EEUU.* http://www.gaceta.es/05-05-2009+corea_norte_se_infiltra_redes_informaticas_ejercito_eeuu,noticia_1img,8,8,55886 . última consulta junio 15 de 2009.

[118] *Report: NKorea Operating Cyber Warfare Unit.* http://abcnews.go.com/International/wireStory?id=7503519 . 2009. última consulta junio 15 de 2009.

3. ALGUNAS POLITICAS DE CIBERDEFENSA EN EL CAMPO INTERNACIONAL

3.1 ESTADOS UNIDOS:

Estados Unidos desde hace unas décadas ha entendido el fenómeno de la información que fluye a través de los medios de comunicación electrónicos, como una poderosa arma de guerra a ser utilizada en su favor.

El concepto de Internet como se conoce hoy día, nació a partir de los desarrollos militares. Esto ha facilitado la creación de una doctrina alrededor de cómo aprovechar y defender su ciberespacio.

La nueva doctrina en asuntos se basa el manejo de operaciones centradas en red y el manejo de una red de información global.

Los Estados Unidos han emitido en la última década directrices y creado instituciones de respuesta primaria para proteger su ciberespacio[119]. En primer lugar en 2003 el presidente George W. Bush firmó la "*Estrategia nacional para asegurar el Ciberespacio*"[120], documento orientado a proteger la infraestructura de tecnologías de información de las cuáles depende su economía, seguridad y forma de vida.

Se acepta el hecho, que defender el ciberespacio es tan complejo que requiere de la participación del gobierno, el sector privado, y el pueblo americano. Esta estrategia se basa en la cooperación entre el sector civil y el gobierno, las alianzas a nivel internacional, el conocimiento permanente de las posibles amenazas y el entrenamiento.

---

[119] LORD, William T. *Comando Ciberespacial de la Fuerza Aérea de Estados Unidos*. Publicado en Air & Space Power Journal. 2009.

[120] *The National Strategy to Secure Cyberspace*. 2003. http://www.au.af.mil/au/awc/awcgate/whitehouse/cyberstrategy.pdf. Última consulta junio 15 de 2009

Luego en 2006 se elabora el documento denominado "*Estrategia Militar Nacional para las Operaciones Ciberespaciales*"[121], orientado a establecer lineamientos a los organismos pertenecientes al departamento de defensa. Se da importancia a las operaciones militares en el ciberespacio, para asegurar la superioridad y dominio a nivel mundial y apoyar los intereses nacionales de los Estados Unidos.

Posteriormente, a comienzos del 2009 la Fuerza Aérea incorporaría dentro de sus misiones las operaciones en el ciberespacio. Para lo cuál se establece el Comando Ciberespacial de la Fuerza Aérea[122], unidad dedicada a ejecutar las operaciones militares de ciberdefensa de Estados Unidos. Esta nueva unidad de desarrollará operaciones de información, guerra electrónica, inteligencia cibernética y guerra en red.

Se han creado dos organismos enmarcados dentro de la división de seguridad interna: El primero es la División de Ciberseguridad Nacional -"NCSD[123]" encargada de mantener un sistema de respuesta nacional en el ciberespacio y proteger la infraestructura crítica de la nación. Y el segundo un Equipo de respuesta a incidentes de seguridad – "US-CERT"[124], encargado de responder a los ataques que se den a entidades gubernamentales.

3.2 OTAN:

En el caso europeo, la OTAN ha tomado el liderazgo de la ciberdefensa de sus países miembros. En 2002 los líderes de los países miembros motivan la creación de un programa de ciberdefensa. El primer paso fue crear el NCIRC (NATO Computer Incident Response Capability), organismo encargado de analizar y compartir información sobre seguridad de la información.

---

[121] *National Military Strategy for Cyberspace Operations.* http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf . última consulta junio 15 de 2009.

[122] *Air Force works to defend cyberspace, too.* http://www.afcyber.af.mil/news/commentaries/story.asp?id=123104768 . última consulta junio 15 de 2009.

[123] *National Cybersecurity Division.* http://www.dhs.gov/xabout/structure/editorial_0839.shtm . última consulta junio 15 de 2009.

[124] *United states computer emergency readines team.* http://www.us-cert.gov/aboutus.html . última consulta junio 15 de 2009.

En 2007 producto de los ataques a Estonia, se creó el Centro de excelencia de cooperación en ciberdefensa (COE), conformado por expertos de España, Alemania, Italia, Eslovaquia, Estonia, Letonia y Lituania. Con el propósito de adelantar programas de investigación y capacitación en ciberguerras y compartir lecciones aprendidas.

3.3 FRANCIA:

Sin embargo este apoyo de la OTAN a sus países miembros, cada uno de ellos de manera independiente y paralela han desarrollado sus programas de ciberdefensa.

Al revisar el último libro blanco de defensa de Francia, emitido en 2008[125], se comienza por reconocer el impacto que la globalización ha tenido en la seguridad internacional. El crecimiento de usuarios de Internet a nivel mundial, que pasará de 16 millones de personas en 1996 a 1500 millones de personas en el 2010[126].

Esto implica para Francia que debe estar preparada para ciberataques provenientes de estados o de otras fuerzas, que atenten contra el modo de vida de sus ciudadanos, las redes vitales de la nación o contras sus capacidades militares.

Promueve un cambio de mentalidad gubernamental, para cambiar de una estrategia de defensa pasiva a una estrategia de defensa activa, ofensiva, de respuesta rápida y de permanente supervisión de las amenazas.

Procede a clasificar los ciberataques con un nivel de alta probabilidad de ocurrencia y desde pequeña a gran escala[127].

---

[125] SARKOZY, Nicolas. *The French white paper on defence and national security*. 2008. http://www.defense.gouv.fr/content/download/134828/1175142/version/1/file/LivreBlancGB.pdf . última consulta junio 15 de 2009.
[126] Ibíd., Pág. 21.
[127] Ibíd. Pág. 54.

Es importante resaltar como Francia hace igual énfasis en la prevención de ciberataques, como en el manejo de la disuasión nuclear y de control de espacio exterior. Procede a crear una nueva agencia responsable de la seguridad de los sistemas de información, bajo la jurisdicción del primer ministro y del ministro de defensa[128].

Se reconoce la posibilidad de las guerras cibernéticas, para lo cuál se proponen cuatro acciones a ejecutar: Creación de un estado mayor conjunto para las acciones de ciberguerra, desarrollar las herramientas tecnológicas a manera de armas digitales, formular una doctrina ofensiva ante los ciberataques y seleccionar y preparar el personal idóneo para tales propósitos.

3.4 BRASIL:

Analizando las recientes políticas de defensa en Latinoamérica, el mejor caso de estudio es el de Brasil como potencia mundial y regional. Adicionalmente por ser un país vecino de Colombia con el cuál se tiene buenas relaciones internacionales.

Brasil en su estrategia nacional de defensa emitida en diciembre del 2008[129], reconoce que se deben generar directrices y fortalecer tres sectores decisivos para la defensa nacional: el cibernético, el espacial y el nuclear.

Con el propósito, que Brasil no dependa de tecnologías extranjeras en lo espacial y cibernético. Hace énfasis en lograr una red de datos segura para la red de comunicaciones con los submarinos, fuerza aérea y terrestre.

Igualmente promueve la capacitación en el uso del ciberespacio en los sectores de la industria, educativo y militar. Para lo cuál impulsa una política de formación de científicos que dominen el ciberespacio, el espacio exterior y lo nuclear.

---

[128] Ibíd. Pág. 174.

[129] *Estrategia nacional de defensa.* http://merln.ndu.edu/whitepapers/Brazil_Portuguese2008.pdf . Pág. 3. última consulta junio 15 de 2009.

Insta a lograr las competencias necesarias en estos tres campos, al nivel de la inteligencia militar. En el ámbito de las relaciones exteriores, promueve desarrollar programas estratégicos con naciones amigas con el ánimo de contribuir a la estabilidad regional. Finalmente promueve el perfeccionamiento de los sistemas de información asociados a la defensa nacional.

Brasil ha implantado un modelo interesante para el Equipo Nacional de Respuesta a Incidentes de seguridad de Computadores. Este modelo es muy interesante porque aunque es una entidad del gobierno, se financia a partir de prestar servicios al sector privado[130].

En el campo de los delitos informáticos, Brasil ha incorporado leyes en su código penal para quiénes alteren o ataquen sistemas del gubernamentales. Pero no penaliza aún a quiénes ataquen sistemas de información del sector privado[131].

4. UN NUEVO MODELO DE LAS ORGANIZACIÓNES PARA LA CIBERDEFENSA.

Las Tecnologías de la Información y las comunicaciones afirman cada vez mas el concepto presentado de la denominada "Aldea Global"[132], bajo el cuál las tradicionales fronteras geográficas de las naciones se reevalúan.

En el Ciberespacio amparados en el concepto de Estado-Nación que agrupa variedad de comunidades bajo un mismo territorio, se presentará el dilema de cuál son nuestros ciudadanos que debemos defender ante las posibles amenazas.

Como se diferencia a los civiles, de los terroristas que amenazan la ciberdefensa nacional.

---

[130] COMISIÓN DE REGULACIÓN DE TELECOMUNICACIONES – República de Colombia. *Recomendaciones al gobierno nacional para la implementación de una estrategia nacional de ciberseguridad.* 2007. Pág. 25.

[131] Ibíd., Pág. 20.

[132] MCLUHAN, Marshall y Bruce R. POWERS. *the global village: Transformations in World life and Media in the 21st century.* Nueva York, Oxford University Press. 1989

Para las instituciones gubernamentales se tornará en casi imposible de controlar y censurar, en el Ciberespacio los flujos de información provenientes de un conflicto.

Al revisar las acciones relacionadas con la ciberdefensa de los países aliados de Estados Unidos como Georgia o Corea del sur, se ve como el gobierno de los Estados Unidos se inclina por fortalecer las capacidades de defensa y a la vez crear la capacidad de disuasión y ataque en caso de ser necesario.

En este mundo cada vez mas las economías se entrelazan, la necesidad de pensar en un modelo de "Defensa en Red" entre las naciones es cada vez mas necesario.

John Arquilla y David Ronfeldt presentan un concepto que se puede ajustar al modelo de Ciberdefensa, y es "guerra de redes".[133] Este concepto ha tomado importancia en la actualidad gracias a los modelos de un mundo interconectado y globalizado.

Anteriormente grupos o comunidades culturalmente y tecnológicamente aislados no tenían la capacidad de intercambiar comunicaciones, ni dar a conocer sus pretensiones o ideas políticas, o de coordinarse y tratar de organizar algún tipo de modelo de comando y control descentralizado[134].

Gracias a las tecnologías de la comunicación esto es posible. Los modelos de trabajo en red se han visto operando en el mundo real, en el cuál se puede ver como se genera mayor sinergía y conocimiento a medida que la red crece y se adapta al contexto en el cuál opera.

---

[133] ARQUILLA, John y David RONFELDT. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch1.pdf . última consulta junio 15 de 2009.

[134] ENAMORADO, Javier J., y José Julio FERNÁNDEZ y Daniel SANSÓ. *Seguridad y defensa hoy. Construyendo el futuro*. Ed. Plaza Valdes. Pág. 48.

En este modelo de operaciones, las capacidades de mando y control se encuentran descentralizadas y no necesitan que otros nodos o células de la red aprueben o desaprueban sus decisiones.

De igual forma el procesamiento de la información se hace manera distribuida y en forma paralela, garantizando que los líderes o iniciadores de la red no se vean congestionados por la tradicional forma piramidal como operan las organizaciones.

En el nuevo modelo de operación en red aplicado en los conflictos armados podríamos decir que hace parte los nuevos modos de operar asimétricos, a los cuales los estados deben enfrentarse.

Esta manera de actuar se puede aplicar de manera natural en el Ciberespacio, lo cuál obliga a pensar en nuevo modo de planear la defensa de las naciones en la era de la información. Igualmente se debe implementar un modelo de defensa en red de las naciones, para contrarrestar los ataques en red que se puedan presentar de manera simultánea contra uno de sus miembros.

Un ejemplo de esta manera de ciber-defensa en red, lo acaba de comenzar a implementar la OTAN, producto del ataque sufrido a Estonia por parte de supuestos hackers rusos. La OTAN recientemente creo un centro de ciberdefensa en Estonia, para el análisis y respuesta a ataques y amenazas procedentes de Internet[135].

En la era industrial se estima que los ejércitos podían mantener sus capacidades operativas en un 30%, pero en el modelo de operación en red se estima que podrán llegar a tener un 70% de bajas y aún tener la capacidad de seguir operando[136].

---

[135] *Siete países de la OTAN harán un centro para la ciberdefensa en Estonia.* Diario El País. 2008. http://www.elpais.com/articulo/Pantallas/paises/OTAN/haran/centro/ciberdefensa/Estonia/elpepirtv/20080516elpepirtv_3/Tes . última consulta junio 15 de 2009.

[136] ENAMORADO, Javier J. Op. cit. Pág. 48

Un ejemplo de adaptación al modelo de trabajo en redes se puede ver en Colombia luego del desmantelamiento del Cartel de Medellín y el Cartel de Cali. La lucha contra el narcotráfico ha obligado a sus integrantes a armar redes de distribución, que operan de manera independientemente. Con el propósito que si una de las rutas cae en poder de las autoridades, toda la estructura no tambalea y colapsa.

Pensando en el modelo de organizaciones para la Ciberdefensa de las naciones, se puede revisar el modelo expresado por Francis Fukuyama y Abram Shulsky [137]. Sostiene que las organizaciones se pueden agrupar en tres formas: Tradicional y jerárquica, Planas y en Red.

No está en desacuerdo que los tres tipos de organización no puedan operara simultáneamente, lo importante es adaptar las organizaciones de defensa para los nuevos retos de las amenazas en red. Existen ciertas decisiones y lineamientos que se deben tomar en el nivel central, pero otras si pueden operar de manera descentralizada.

Los ejércitos se podrían percibir como organizaciones que operan tradicionalmente de forma jerárquica. Pero al ver el modo como organizó Napoleón su ejercito para las campañas se ve como el mismo comandaba sus divisiones de manera simultánea sin intermediarios. De igual forma se vio en la segunda guerra mundial con sus formaciones de tanques denominados "BlitzKrieg" que operaban de manera independiente, pero coordinadas por radios de comunicaciones.

Peter Drucker expreso una frase que definió un nuevo modelo corporativo y es la "Organización basada en la información" [138]. El autor propone que las organizaciones deben estar compuestas principalmente por especialistas quiénes dirigen y se orientan, en base a la retroalimentación de sus colegas, clientes y casa matriz. Bajo este paradigma

---

[137] FUKUYAMA, Francis y Abram N. SHULSKY. *The "Virtual Corporation" and Army Organization.* http://www.rand.org/pubs/monograph_reports/2007/MR863.pdf . última consulta junio 15 de 2009.

[138] DRUCKER, Peter F. *Drucker su visión sobre: la administración, la organización basada en la información, la economía, la sociedad.* Ed. Norma, 1996.

propone organizar pequeños cantidades de empleados altamente capacitados para producir bienes y servicios con una alta capacidad de adaptación.

5. REVISION DE LAS ACCIONES ENCAMINADAS A FORTALECER LA CIBERDEFENSA EN COLOMBIA.

Colombia como nación que no se ha aislado de los procesos de globalización. Como una nación que hace parte de los procesos de intercambio de información a nivel global, deberá comprender el ciberespacio. Con el propósito de poder dominarlo y así poder definir una correcta política para su defensa. Para cumplir con el objetivo de garantizar la libertad de acción y movimiento por parte de los ciudadanos colombianos, se deben construir las capacidades y habilidades para su dominio, al igual que sus amenazas y vulnerabilidades.

Se podría pensar en Colombia como un país del tercer mundo, donde se evidencia el uso de la realpolitk como herramienta de solución al conflicto interno. Por lo cuál, no tendría sentido preocuparse por el uso de la noopolitik por parte de otras naciones u organizaciones contra Colombia en el Ciberespacio.

Pero al revisar las cifras de penetración y uso de la tecnologías de la información, se puede ver como los ciudadanos colombianos cada vez ejercen el derecho a la información: cerca de 33 millones de teléfonos celulares activos en el país, y se estima que para finales del 2009 unos 40 millones de celulares. La penetración de Internet en Colombia es de un 28%, por encima del Perú con un 27% y por debajo de Venezuela con un 55%[139].

En el aspecto de seguridad informática, según la última encuesta de seguridad informática elaborada en Colombia en mayo del 2008[140], los sectores mas amenazados son el

---

[139] *El 45% de los colombianos tiene un PC en las zonas urbanas*. Diario El Tiempo. 2009. http://www.eltiempo.com/enter/actualidad_a/home/el-45-de-los-colombianos-tiene-un-pc-en-las-zonas-urbanas_4762394-1 . última consulta junio 15 de 2009.

[140] ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS. *VIII Encuesta Nacional de Seguridad Informática.* Bogotá. 2009.

financiero, la educación, la industria informática, las telecomunicaciones y el gobierno. El actual gobierno en el documento Visión 2019 del Departamento Nacional de Planeación, plantea como metas alcanzar una penetración cercana al 60% de la población[141]. De igual forma, lograr que el 100% de las entidades gubernamentales estén interconectadas.

En el aspecto legal el gobierno ha venido fortaleciendo la normatividad en el aspecto de los delitos informáticos, labor desarrollada por en el Ministerio del Interior y de Justicia.

Producto esta labor es a reciente ley 1273 de 2009[142], la cuál adicionó nuevos delitos: acceso abusivo a un sistema informático sin autorización o por fuera de lo acordado, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios Web para capturar datos personales, hurto por medios informáticos y semejantes, y transferencia no consentida de activos.

Colombia a nivel defensivo, con el apoyo del Ministerio de Relaciones Exteriores y la OEA planea crear el centro de respuestas a incidentes informático. El cuál fue nombrado CIRTISI Colombia (Centro de Información y Respuesta Técnica a Incidentes de Seguridad Informática de Colombia)[143].

Las recomendaciones de la Comisión de Regulación de las Telecomunicaciones – CRT, consideran que al evaluar el modelo de Brasil sería el más adecuado de implementar. Porque aunque es una entidad creada y regulada por el gobierno, su financiación se logra a partir de prestar servicios al sector privado

---

http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/19-VIIIEncuestaNacionalSeguridadInformatica.pdf . , última consulta febrero 23 de 2009.

[141]DEPARTAMENTO NACIONAL DE PLANEACION. *Avanzar hacia una sociedad mejor informada.* 2008 http://www.dnp.gov.co/PortalWeb/Portals/0/archivos/documentos/2019/Documentos/Documento%20SOCIEDAD%20MEJOR%20INFORMADA.pdf, última consulta febrero 23 de 2009.

[142] SENADO DE LA REPUBLICA DE COLOMBIA. *Ley 1273 de 2009. Congreso de la república.*. 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html . última consulta febrero 23 de 2009

[143] COMISIÓN DE REGULACIÓN DE TELECOMUNICACIONES – REPÚBLICA DE COLOMBIA. Op. Cít. Pág. 25.

Se han comenzado a generar acciones para colaborar con el sector privado en las labores de toma de conciencia que la seguridad informática de la nación, no es responsabilidad del estado sino también del sector privado y de sus ciudadanos.

CONCLUSIÓN

Colombia como estado debe lograr alcanzar las competencias y capacidades necesarias para llevar a cabo operaciones de defensa y de disuasión en el ciberespacio. Se requiere para ello un alto nivel de cooperación interagencias gubernamentales y privadas para lograr los niveles óptimos deseados.

Colombia ya ha comenzado a adelantar pasos en la obtención de las capacidades de reacción en caso de posibles ataques, para ello adelanta las labores de un centro de respuesta CERT apoyado por la OEA.

Retomando la frase del General Miguel Alonso Baquer: "En tiempos de incertidumbre, de lo que hay que disponer es de unos ejércitos polivalentes y flexibles"[144]. Aplicado a las fuerzas militares de Colombia, se podría sugerir una adaptación de su organización para enfrentar las nuevas amenazas provenientes de organizaciones que operan en un esquema en red.

Este argumento se puede enmarcar dentro del pensamiento expresado por Alejo Vargas, cuando habla de la modernización de la fuerza publica. Sugiere que se debe trabajar en mejorar las condiciones de movilidad y reacción rápida, y la formación de fuerzas especializadas para responder al terrorismo[145].

Las nuevas fuerzas militares se deben adaptar para contrarrestar los nuevos modelos de operación de las redes de terroristas internacionales. Estas redes pueden intercambiar

---

[144] VARGAS, Alejo. Op. Cit. Pág. 441.
[145] VARGAS, Alejo. Op. Cit. Pág. 368.

conocimiento y nuevas formas de ataque, gracias a que actúan en base a modelos globalizados.

Los organismos de defensa de Colombia se enfrentan a un reto y es el de cómo operar eficientemente en red, para contrarrestar las posibles amenazas al ciberespacio. Se puede decir que la mejor forma de luchar contra redes es operar en forma de red.

La evolución de las FARC a las redes internacionales diplomáticas[146], la influencia en culturas europeas como el caso de las camisetas de las FARC en Dinamarca[147], y la comercialización de uranio[148], entre otros muchos. Demuestran como día a día, van desarrollando la capacidad de adaptación y de aprendizaje del nuevo entorno mundial. Los computadores del cabecilla de las FARC - Raúl Reyes. Son un ejemplo de sus capacidades de establecer capacidades de comando y control, con base en otros territorios.

Las FARC posiblemente, no han desarrollado las capacidades para un ciberataque al ciberespacio de Colombia. Pero si se les da tiempo, las pueden desarrollar y así fortalecer su capacidad de ejercer poder blando.

Colombia debe comenzar un programa de reclutamiento y entrenamiento de personal que tengan las habilidades necesarias para defender su ciberespacio

Se recomienda para Colombia la creación de una división de fuerzas especiales para el ciberespacio, con el propósito de garantizar de manera preventiva y reactiva la seguridad de los activos estratégicos de la nación en el ciberespacio. Colombia debe estar preparado

---

[146]ARRÁZOLA, María del Rosario. *La diplomacia de las FARC.* http://www.elespectador.com/impreso/farc/articuloimpreso-diplomacia-de-farc . última consulta junio 15 de 2009.

[147] REVISTA SEMANA. *Ratifican condena a seis daneses por camisetas de las Farc.* http://www.semana.com/noticias-mundo/ratifican-condena-seis-daneses-camisetas-farc/122081.aspx . última consulta junio 15 de 2009.

[148]DIARIO EL ESPECTADOR. *El uranio de las FARC.* http://www.elespectador.com/impreso/cuadernilloa/judicial/articuloimpreso-el-uranio-de-farc . , última consulta junio 15 de 2009.

desde ya para posibles conflictos, se puede ver como conflictos del mundo real tiene su equivalente en el ciberespacio.

En Estados Unidos y China adelantan competencias y concursos al interior de las universidades, orientados a la ciberdefensa. Proceso durante el cuál se va seleccionado personal que tiene la habilidad para poder enfrentarse a estas nuevas amenazas.

Otra alternativa viable es la poder aprovechar parte del personal de la reserva activa para prepararlos para monitorear actividades en la red, que actúen como evangelizadores de las mínimas técnicas de ciberseguridad de los empleados del gobierno y sector privado, y en caso de un eventual amenaza puedan apoyar en las labores de disuasión y mitigación del evento que se llegue a presentar.

El poder blando y la noopolitik se convierten en activos estratégicos de las naciones, los cuáles ayudan a su desarrollo. Se debe propender por un ciberespacio compartido pero a la vez seguro. Se debe crear una nueva doctrina para el manejo de la información estratégica en el ciberespacio de Colombia. Para poder regular las situaciones en caso de crisis, conflictos o potenciales amenazas a la ciber-seguridad nacional.

Las alianzas multilaterales, son factores de éxito demostrados en la lucha contraterrorista. Nuestros posibles enemigos en el ciberespacio, pueden estar localizados en cualquier nación. Y tratar de mitigar estas amenazas no es tarea de un solo país.

La Ciberdefensa Nacional de Colombia debe tener en cuanta la protección de sus activos estratégicos y críticos, tanto civiles como gubernamentales y militares. Debe fortalecer continuamente la lucha contra el cibercrimen y los delitos informáticos.

Al revisar la política de Seguridad Democrática y la actual política de consolidación, se hace evidente la tesis que Colombia ha esta centrado eminentemente en el conflicto interno.

Gracias a la creciente penetración de las tecnologías de información y comunicación, se hace necesario que dentro de las políticas de defensa de Colombia se debe agregar un capítulo dedicado a la Ciberdefensa.

Finalmente, la falta de inclusión de una política de ciberdefensa dentro del marco una política de defensa nacional, es una gran oportunidad para se implementada y potenciada.

CONCLUSIONES

En el nuevo campo de batalla del Ciberespacio son varias los fundamentos de la lógica estratégica, que se pueden aplicar como instrumentos de uso del poder: la Negación, la Interferencia y el uso de la influencia representado en el Poder Invisible (Soft Power).

Diseñar una buena política de seguridad nacional del ciberespacio servirá de base para el planeamiento y desarrollo de operaciones de información en época de paz y de tensiones.

Probablemente los países en el siglo XXI se enfocarán más en hacer parte de los procesos de globalización, que en disputar los espacios geográficos. Se prevé entonces, que las guerras de cuarta y quinta generación estarán a la orden del día.

Bajo estas perspectivas el nuevo centro de gravedad para las guerras cibernéticas, son las redes de información.

Colombia como Estado debe estar preparada para conquistar y tomar un papel de liderazgo, en el Ciberespacio. De igual forma debe estar preparada para defenderlo de posibles enemigos que deseen vulnerar sus intereses.

El gobierno colombiano debe entonces diseñar una estrategia nacional para la defensa y seguridad del ciberespacio. Esta estrategia debe ir encaminada a defender a Colombia de posibles ataques contra los intereses nacionales que se perpetren o planean aprovechando la red Internet.

Se debe entonces, inscribir como parte de los intereses nacionales la presencia y protección del ciberespacio colombiano.

Colombia como estado debe lograr alcanzar las competencias y capacidades necesarias para llevar a cabo operaciones de defensa y de disuasión en el ciberespacio. Se requiere para ello

un alto nivel de cooperación entre agencias gubernamentales y privadas para lograr los niveles óptimos deseados.

Se recomienda impulsar aún mas la investigación y el desarrollo (I+D) tecnológico, particularmente en las áreas de informática y telecomunicaciones.

Colombia debe comenzar un programa de reclutamiento y entrenamiento de personal que tengan las habilidades necesarias para defender su ciberespacio

Se recomienda para Colombia la creación de una división de fuerzas especiales para el ciberespacio, con el propósito de garantizar de manera preventiva y reactiva la seguridad de los activos estratégicos de la nación en el ciberespacio.

En Colombia gracias a la cooperación militar con los Estados Unidos y la dinámica del conflicto interno, ya se ha evidenciado el uso de las tecnologías de información y comunicaciones a nivel operacional. Tal es el caso, de las bombas inteligentes empleadas en operaciones contra cabecillas de las FARC, como el "Negro Acacio" y "Raúl Reyes".

La ciberguerra también se emplea actualmente en el conflicto interno colombiano. Esto se evidencia en el empleo de aviones de inteligencia no tripulados que envían sus transmisiones de video en tiempo real, ha facilitado la toma de decisiones en corto tiempo. Tecnologías de información, que permiten en tiempo real captar comunicaciones de la guerrilla, monitorear conversaciones telefónicas y correos electrónicos vía Internet. Este uso de la tecnología de comunicaciones en esta clase de conflicto asimétrico, ha obligado a que las FARC retornen al empleo de correos humanos.

Operaciones de información en Internet como la empleada en la operación Jaque, donde a las FARC se les hizo crear que la organización "Misión Internacional Humanitaria" era real. Acudiendo al método de montar una página oficial de la misión en Internet que se

encontraba hospedada en la dirección http://misionhi.org/. Reafirman la tesis que el ciberespacio se ha convertido en un nuevo espacio de batalla.

Las fuerzas armadas del siglo XXI tendrán como reto aprovechar las ventajas estratégicas que presenta la era de la información, ante los modelos actuales de organizaciones regidas aún por la era industrial. En la era de la información, las amenazas difieren de las de la era industrial. Muchas de ellas no se pueden atacar con tácticas militares convencionales.

Actualmente gracias a los procesos de modernización tecnológica, se puede afirmar que las Fuerzas Militares colombianas cuentan con un sistema de comando, control, y comunicaciones, que permite a nivel estratégico conducir operaciones de manera coordinada y eficiente. Sin embargo, es recomendable para Colombia continuar con el proceso de fortalecimiento y modernización de los sistemas C3. No solo pensando en función del conflicto interno, sino para la defensa de la nación en caso de amenazas externas o de procesos de cooperación internacional en la fase de postconflicto.

Como parte del proceso de modernización de las FFMM colombianas, se han implementado comandos conjuntos, apoyados por el comando y control unificado. Los cuáles han incrementando el poder de combate. Contribuyendo a que los narcoterroristas de las FARC, hayan perdido gran control sobre el territorio que antiguamente dominaban. Generando indisciplina táctica y pérdida de mando y control sobre las unidades de las FARC.

Esta monografía sirve de base para desarrollar una posterior investigación centrada en el efecto de las tecnologías de información y comunicaciones en el conflicto armado en Colombia. Tanto del lado de los grupos armados al margen de la ley, como del lado de las Fuerzas Militares colombianas.

Adicionalmente puede generarse una investigación a fondo de los efectos políticos del uso del ciberespacio, como un nuevo campo del ejercicio de las políticas de defensa de las

naciones. Ya que en la era de la información las nuevas formas de guerra, necesitan idear nuevas reglas que las ayuden a regularse.

BIBLIOGRAFIA

ADAMS, K. *La próxima guerra mundial*, Editorial Granic, Madrid, 2001.

ALBERTS, David S. Hayes, Richard E. *Command Arrangements for Peace Operations*. Washington, DC. CCRP Publication Series.

ALBERTS, David S. *Network centric warfare : developing and leveraging information superiority*. Washington, DC. CCRP Publication Series. 2000.

ALBERTS, David S. Hayes, Richard E. *Power to the Edge. Command...Control...in the Information Age*. Washington, DC. CCRP Publication Series. 2000.

AMSTUTZ, Mark R. *La ética de la fuerza*. Oxford, Rowman & Littlefield. 1999.

APPLEBERRY, James. *National and local forces at work Challenging times for creative people*, 1998.

BARNETT,Jeffery R. *Future War: An Assessment of Aerospace Campaigns in 2010.*Air University Press, 1996.

BERKOWITZ, Bruce. *The new face of war, How war will be fought in the 21st Century*. New York, Ed. Free Press. 2003.

BRZEZINSKI, Zbigniew. *Between Two Ages*, Nueva York, Viking Press, 1969.

BUSH, George. *The Deployment of US Armed Forces to Saudi Arabia*, discurso del 8 de agosto de 1990.

CARVAJAL, Leonardo, *"Tres años del gobierno Uribe (2002-2005): Un análisis con base en conceptos dicotómicos de política exterior"*, en OASIS, N.11, Bogotá: Centro de Investigaciones y Proyectos Especiales (CIPE) de la Universidad Externado de Colombia, 2005-2006.

CLAUSEWITZ, Karl Von, *De la guerra*, Ed. La Esfera De Los Libros. 2005

COMISIÓN DE REGULACIÓN DE TELECOMUNICACIONES – República de Colombia. *Recomendaciones al gobierno nacional para la implementación de una estrategia nacional de ciberseguridad*. 2007.

CRAIG, Deare. *Panel: Mexico and the Hemispheric Security Agenda. El Comando Norte de los Estados Unidos Implicancias para la Seguridad y Defensa de México*. Center for Hemispheric Defense Studies. 2003.

CREVELD, Martin. *Command in War*, Cambridge. Howard University Press, 1985.

DRUCKER, Peter F. *Drucker su visión sobre: la administración, la organización basada en la información, la economía, la sociedad.* Ed. Norma, 1996.

ENAMORADO, Javier J., y José Julio FERNÁNDEZ y Daniel SANSÓ. *Seguridad y defensa hoy. Construyendo el futuro*. Ed. Plaza Valdés. 2008

FEAL, Javier. *El poder mediático*, en Boletín No.283, CESEDEN – Ministerio de Defensa de España. 2004.

FLORES, María Lourdes. *Internet como herramienta del integrismo Yihadista*. Publicado en el Boletín No.303, CESEDEN – Ministerio de Defensa de España. 2004,

Fundación Seguridad y Democracia. *Fuerzas Militares para la guerra. La agenda pendiente de la reforma militar.* Bogotá, 2003.

GIBSON, William. *Neuromancer*. Ace Books, 1984

HOWARD, Michael. Paret, Peter. *Carl von Clausewitz: On War.* Princeton, NJ. Princeton University Press, 1989,

JOINT CHIEFS OF STAFF. *Unified Action Armed Forces.* Washington, D.C., Joint Pub,1995.

KEEGAN, John. *The Mask of Command*. Penguin Books, 1987

KEPEL, G., *La yihad. Expansión y declive del islamismo*. Barcelona, Ediciones Península, 2000.

LORD, William T. *Comando Ciberespacial de la Fuerza Aérea de Estados Unidos.* Publicado en Air & Space Power Journal. 2009.

MCLUHAN, Marshall y Bruce R. POWERS. *the global village: Transformations in World life and Media in the 21st century.* Nueva York, Oxford University Press. 1989.

NYE, Joseph S. y William A. OWENS, *America's Information Edge*, Foreign Affairs, vol. 75, N° 2. 1996.

NYE, Joseph S., *La paradoja del poder norteamericano*. Madrid, Taurus, 2003.

RICE, Condoleezza. *The Party, the Military, and Decision Authority in the Soviet Union.* World Politics. Vol. 40, No. 1. 1987.

ROMAN, Gregory A. *The Command or Control Dilemma: When Technology and Organizational Orientation Collide*. Air War College Maxwell .1996.

ROSALES, Gustavo. *Geopolítica y geoestrategia liderazgo y poder · Ensayos ·*. Universidad Militar Nueva Granada, 2005.

SANCHEZ, Pedro. *Guerras de Cuarta Generación y las Redes*. Revista Ejercito No.812. Madrid. 2008.

SCHLÖGEL, Karl. *En el Espacio Leemos el Tiempo. Sobre Historia de la Civilización y Geopolítica.* Traducido por José Luis Arántegui. Publicado por Siruela, 2007.

SPROLES, Noel. *Command and Control as a process. Establishing Measures of Effectiveness for Command and Control: A Systems Engineering Perspectiva.* University of South Australia. 2001.

SPROLES, Noel. *Establishing Measures of Effectiveness for Command and Control: A Systems Engineering Perspectiva.* University of South Australia.2001.

SUN TZU. *El arte de la guerra.* Traducido por Samuel B. Griffith. Oxford University Press, New York, 1963.

TODD, Greg. *C1 Catharsis*. Army War College, 1986.

TOFFLER, Alvin y Heidi, *Las guerras del futuro*, Editorial Plaza & Janes, 1998.

VARGAS, Alejo. *Las fuerzas armadas en el conflicto colombiano. Antecedentes y perspectivas*. Bogotá. Intermedio Editores. 2002.

YATES, Benjamin. *The past and present as a window on the future*. New York. Oxford University Press. 1991.

Referencias de medios electrónicos:

Air Force works to defend cyberspace, too. http://www.afcyber.af.mil/news/commentaries/story.asp?id=123104768 . Última consulta junio 15 de 2009.

ALBARRÁN, Gerardo. *La guerra mediática.* Sala de Prensa. http://www.saladeprensa.org/art283.htm. Última consulta Noviembre 22 de 2008.

ALBON, Chris. *Colombian Hostage Rescue Could Have Been Foiled By A Single Internet Search.* 2008. http://warandhealth.com/colombian-hostage-rescue-could-of-been-discovered-by-a-single-internet-search/ . Última consulta Noviembre 22 de 2008.

ANGELONE, Juan Pablo. *Doctrina de la Seguridad Nacional y Terrorismo de Estado: Apuntes y Definiciones*. http://infoderechos.org/es/node/178. Última consulta junio 15 de 2009.

ARQUILLA, John y David RONFELDT, *The Emergence of Noopolitik*. National Defense Research Institute-RAND, 1999. http://www.rand.org/pubs/monograph_reports/MR1033/MR1033.sum.pdf . Última consulta junio 15 de 2009.

ARQUILLA, John y David RONFELDT. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch1.pdf . Última consulta junio 15 de 2009.

ARRÁZOLA, María del Rosario. *La diplomacia de las FARC*. http://www.elespectador.com/impreso/farc/articuloimpreso-diplomacia-de-farc. Última consulta junio 15 de 2009.

ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS. *VIII Encuesta Nacional de Seguridad Informática*. Bogotá. 2009. http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/19-VIIIEncuestaNacionalSeguridadInformatica.pdf . Última consulta febrero 23 de 2009.

Ataque a la Embajada china: fue un error de información de la CIA. Diario El Clarín. 1999 http://www.clarin.com/diario/1999/05/10/i-02801d.htm . Última consulta Noviembre 22 de 2008.

ASSER, Martin. *Echelon: Big brother without a cause?*. BBC News. 2000. http://news.bbc.co.uk/2/hi/europe/820758.stm. Última consulta Febrero 22 de 2009.

Auto de levantamiento parcial del sumario, Documentos 11-M Madrid. http://www.elmundo.es/documentos/2004/03/espana/atentados11m/documentos.html. Última consulta Febrero 22 de 2009.

Avanzar hacia una sociedad mejor informada. Departamento Nacional de Planeación. http://www.dnp.gov.co/PortalWeb/Portals/0/archivos/documentos/2019/Documentos/Documento%20SOCIEDAD%20MEJOR%20INFORMADA.pdf, Última consulta febrero 23 de 2009.

BARRERA H., Guillermo. La *importancia de las operaciones conjuntas, coordinadas y combinadas de la Armada Nacional*. http://www.armada.mil.co/?idcategoria=537943. Última consulta Noviembre 22 de 2008.

BILLO, Charles G. y Welton CHANG. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* . Pág. 14. http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf. Última consulta junio 15 de 2009.

CARACOL RADIO. *El 'Virus Medellín' causa estragos en los computadores de Santander* http://www.caracol.com.co/nota.aspx?id=666183 Última consulta Octubre 11 de 2008.

Castro: a threat to the security of the united states. http://www.globalsecurity.org/wmd/library/news/cuba/oagmc020.htm. Última consulta Octubre 11 de 2008.

Chávez pide alianza militar contra EE.UU. http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7212000/7212793.stm Última consulta Octubre 11 de 2008.

CNN. *Gulf War strikes marked a sea change in air tactics.* http://www.cnn.com/SPECIALS/2001/gulf.war/legacy/airstrikes/index.html. Última consulta Noviembre 22 de 2008.

Corea del Norte se infiltra en las redes informáticas del Ejército de EEUU. http://www.gaceta.es/05-05-2009+corea_norte_se_infiltra_redes_informaticas_ejercito_eeuu,noticia_1img,8,8,55886 . Última consulta junio 15 de 2009.

DEPARTAMENTO NACIONAL DE PLANEACION. *Avanzar hacia una sociedad mejor informada.* 2008 http://www.dnp.gov.co/PortalWeb/Portals/0/archivos/documentos/2019/Documentos/Documento%20SOCIEDAD%20MEJOR%20INFORMADA.pdf. Última consulta febrero 23 de 2009.

DEPARTMENT OF THE NAVY - NAVAL HISTORICAL CENTER. *War Chronology: January 1991.* http://www.history.navy.mil/wars/dstorm/dsjan2.htm. Última consulta Noviembre 22 de 2008.

DIARIO EL ESPECTADOR. *El uranio de las FARC.* http://www.elespectador.com/impreso/cuadernilloa/judicial/articuloimpreso-el-uranio-de-farc . Última consulta junio 15 de 2009.

DIARIO EL PAÍS. *Siete países de la OTAN harán un centro para la ciberdefensa en Estonia.* 2008. http://www.elpais.com/articulo/Pantallas/paises/OTAN/haran/centro/ciberdefensa/Estonia/elpepirtv/20080516elpepirtv_3/Tes . Última consulta junio 15 de 2009.

DIARIO EL TIEMPO. *El 45% de los colombianos tiene un PC en las zonas urbanas.* 2009.

http://www.eltiempo.com/enter/actualidad_a/home/el-45-de-los-colombianos-tiene-un-pc-en-las-zonas-urbanas_4762394-1. Última consulta junio 15 de 2009.

DIARIO EL TIEMPO. *Colombia, el país menos pirata de la región* . Diario El Tiempo. 2008. http://www.eltiempo.com/tecnologia/enter/actualidad_a/home/colombia-el-pais-menos-pirata-de-la-region_4178223-1. Última consulta Octubre 11 de 2008.

El Mundo. *Microsoft suspende el 'Messenger' en los países embargados por EEUU. 2009.* http://www.elmundo.es/elmundo/2009/05/26/navegante/1243360629.html . última consulta junio 16 de 2009.

Estrategia nacional de defensa. http://merln.ndu.edu/whitepapers/Brazil_Portuguese2008.pdf . Última consulta junio 15 de 2009.

Estrategia Nacional para Asegurar el Espacio Cibernético. www.whitehouse.gov/pcipb. Última consulta Octubre 11 de 2008.

FUKUYAMA, Francis y Abram N. SHULSKY. *The "Virtual Corporation" and Army Organization.* http://www.rand.org/pubs/monograph_reports/2007/MR863.pdf . Última consulta junio 15 de 2009.

Guerra entre Rusia y Georgia pasó del terreno de batalla a portales de Internet. http://www.portafolio.com.co/bienestar/cienciaytecnologia/2008-08-14/ARTICULO-WEB-NOTA_INTERIOR_PORTA-4445060.html . Última consulta junio 15 de 2009

GLASSER, S. y S. Coll, *The Web as Weapon.* publicado en The Washington Post. 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html. Última consulta Febrero 22 de 2009.

GOLDSTEIN, Frank I. *Las Operaciones Psicológicas la Guerra del Golfo Pérsico.* Air & Space Power Journal.1996. http://www.airpower.au.af.mil/apjinternational/apj-s/1996/3trimes96/goldstein.html. Última consulta Noviembre 22 de 2008.

GOMPERT, David C., "*Right Makes Might: Freedom and Power in the Information Age*," capítulo 3 en Zalmay Khalilzad, John P. White, Andrew W. Marshall, *Strategic Appraisal: The Changing Role of Information in Warfare*. Informe RAND MR-1016-AF, 1999. http://www.rand.org/publications/MR/MR1016/MR1016.chap3.pdf. Última consulta Octubre 11 de 2008.

GUTIÉRREZ, Víctor Manuel. *Espacio y Geopolítica.* http://mapppcolsan.blogspot.com/2008/06/espacio-y-poltica.html. Última consulta Febrero 22 de 2009.

HANSEL, Mischa. *Challenging Regional Power and Security: Conflicts in Space and Cyberspace*. 2009. http://www.dgap.org/midcom-serveattachmentguid-1de451acbc2880e451a11de80a70dfed144ae4dae4d/2009_dgapbericht-14_nfc-2008_www.pdf. Última consulta junio 15 de 2009

Intelligence and Security Comittee (2006), Report into the London Terrorist Attacks on 7 July 2005., http://www.official-documents.gov.uk/document/cm67/6785/6785.pdf. Última consulta Febrero 22 de 2008.

JARAMILLO, Carlos Eduardo. *FARC están cambiando de estrategia. Revista CAMBIO. 2008.* http://www.cambio.com.co/paiscambio/813/ARTICULO-WEB-NOTA_INTERIOR_CAMBIO-4780133.html. Revista CAMBIO. Última consulta Noviembre 22 de 2008.

LIND, William S. *Fourth Generation Warfare: Another Look.* http://www.d-n-i.net/fcs/4GW_another_look.htm. Última consulta Noviembre 22 de 2008.

LEWIS, James A. *The Architecture of Control: Internet Surveillance in China*, http://www.csis.org/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf. Última consulta junio 15 de 2009.

Ministerio de Defensa Nacional. *Las FARC en el peor momento de la historia.* http://www.mindefensa.gov.co/descargas/Documentos_Home/Farc_el_peor_momento_de_la_historia.pdf. Última consulta Noviembre 22 de 2008.

National Military Strategy for Cyberspace Operations. http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf . última consulta junio 15 de 2009.

NATO launches cyber defence centre in Estonia, acceso en http://en.kioskea.net/actualites/nato-launches-cyber-defence-centre-in-estonia-10374-actualite.php3 . Última consulta Octubre 11 2008.

NATO opens new centre of excellence on cyber defence. http://www.nato.int/docu/update/2008/05-may/e0514a.html . última consulta junio 15 de 2009.

NORTH ATLANTIC TREATY ORGANISATION. *Exploring New Command and Control Concepts and Capabilities*. www.rta.nato.int. 2007. Última consulta Noviembre 22 de 2008.

NYE, Joseph S. Jr., y William A. OWENS, *America's Information Edge*, Foreign Affairs, Marzo/Abril 1996. http://usinfo.state.gov/journals/itgic/0996/ijge/gjcom6.htm . Última consulta Noviembre 22 de 2008.

Radio Nacional de Venezuela. *Listo satélite venezolano Simón Bolívar que expandirá telecomunicaciones.* 2008. http://www.rnv.gov.ve/noticias/index.php?act=ST&f=14&t=79301. Última consulta Octubre 11 de 2008.

Report: NKorea Operating Cyber Warfare Unit. http://abcnews.go.com/International/wireStory?id=7503519 . 2009. última consulta junio 15 de 2009.

Reporters without Borders, The 15 Enemies of the Internet and other Countries to Watch, http://www.rsf.org/print.php3?id_article=15613 . última consulta junio 15 de 2009

REVISTA SEMANA. *Ratifican condena a seis daneses por camisetas de las FARC.* http://www.semana.com/noticias-mundo/ratifican-condena-seis-daneses-camisetas-farc/122081.aspx . Última consulta junio 15 de 2009.

ROGERS, A.P.V. *Una guerra sin víctimas.* Revista Internacional de la Cruz Roja No. 837. 2000. Pág. 165. http://www.icrc.org/web/spa/sitespa0.nsf/html/5TDNZD. Última consulta Noviembre 22 de 2008 .

Russian hackers continue attacks on Georgian sites. http://www.wjla.com/news/stories/0808/543487.html. 2008. Última consulta junio 15 de 2009

SARKOZY, Nicolas. *The French white paper on defence and national security.* 2008. http://www.defense.gouv.fr/content/download/134828/1175142/version/1/file/LivreBlancGB.pdf . Última consulta junio 15 de 2009.

SANZ, Juan C. *El régimen de Sadam prosigue la 'limpieza étnica' contra los kurdos de Irak.* Diario El País. 2003. http://www.elpais.com/articulo/internacional/regimen/Sadam/prosigue/limpieza/etnica/kurdos/Irak/elpepiint/20030305elpepiint_4/Tes/ . Última consulta Noviembre 22 de 2008.

SENADO DE LA REPUBLICA DE COLOMBIA. *Ley 1273 de 2009. Congreso de la república..* 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html . Última consulta febrero 23 de 2009

SHINER, John F. *Reflections on Douhet the classic approach.* Air University Review, 1986. http://www.airpower.au.af.mil/airchronicles/aureview/1986/jan-feb/shiner.html. Última consulta julio 15 de 2009.

SOUTH AMERICA. http://www.internetworldstats.com/south.htm . Última consulta Octubre 7 2008.

Symantec Global Internet Security. Threat Report Trends for July–December 07. Volumen XII, 2008. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf . Última consulta Octubre 7 2008.

TELEGEOGRAPHY. *Global Internet Map* , 2009. www.telegeography.com/products/map_internet/wallpaper/InternetMap09_wall2.jpg, Última consulta Febrero 22 de 2009.

The National Strategy to Secure Cyberspace. 2003. http://www.au.af.mil/au/awc/awcgate/whitehouse/cyberstrategy.pdf. Última consulta junio 15 de 2009

United States Central Command (USCENTCOM). http://www.centcom.mil/. Última consulta Noviembre 22 de 2008.

United states computer emergency readines team. http://www.us-cert.gov/aboutus.html . Última consulta junio 15 de 2009.

US DEPARTMENT OF DEFENSE. *The national military strategy for cyberspace operations*, 2006. http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf. Última consulta junio 15 de 2009

US DEPARTMENT OF HOMELAND SECURITY. *National Cybersecurity Division.* http://www.dhs.gov/xabout/structure/editorial_0839.shtm . Última consulta junio 15 de 2009.

VENTURA, Holly E. *Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power.* Critical Criminology .2005. http://www.cas.sc.edu/socy/faculty/deflem/zgovernterror.html. Última consulta Febrero 22 de 2009.

Visión conjunta 2020: Las fuerzas armadas de los Estados Unidos preparándose para el futuro. http://usacac.army.mil/cac/milreview/spanish/NovDec01/jointvision.PDF. Última consulta Octubre 11 de 2008

WEIMANN, Gabriel. *www.terror.net How Modern terrorism uses the Internet.* publicado en United States Institute of Peace – Special Report. http://www.usip.org/pubs/specialreports/sr116.pdf. Última consulta Febrero 22 de 2008.

WILSON, Clay. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* http://www.ipmall.info/hosted_resources/crs/RL32114_080129.pdf . Última consulta junio 15 de 2009.