ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA

“Guerra de la Información”

TÍTULO

“La influencia de la Guerra de la Información en un Teatro de Operaciones”

Alumno: Mayor (FAA)Eduardo Juan RIQUELME

Tutor:

Año2012

Tabla de Contenidos

RESUMEN ..... **II**

PALABRAS CLAVES ..... **II**

2. Introducción **1**

3. Capitulo I: Evolución de la guerra de la Información **4**

4. Capitulo II: Ámbitos para llevar a cabo la guerra de la información. **11**

Principios de la Guerra de la Información. **14**

Operaciones de Guerra de la Información. **15**

Aplicaciones de Guerra de la Información. **24**

Centros de Gravedad. **25**

Teoría de los Cinco Anillos **25**

5. Conclusiones. **29**

6. Bibliografía **31**

Manuales **31**

Libros **31**

Documentos electrónicos **32**

RESUMEN

La Revolución en Asuntos Militares, definida como la influencia de la tecnología en las guerras, ahora se define en este ámbito como la Guerra de la Información.

Cuando se habla de Guerra de Información se refiere no solo a períodos de conflicto violento, sino también a épocas de paz. Por tanto la Guerra de Información ocurre dentro y fuera de un Teatro de Operaciones.

No obstante, poco interés se ha puesto en referirse específicamente a la Guerra de Información dentro de un Teatro de Operaciones. Se lo asocia frecuentemente con actividades de velo y engaño, pero ese es un concepto de generaciones anteriores de guerra.

En este trabajose analiza la Guerra de la información dentro de un Teatro Operaciones haciendo hincapié en cómo esta nueva forma de combate puede cambiar el desarrollo de las operaciones influyendo directamente tanto en la toma de decisiones de un Comandante de teatro como así también en la capacidad y voluntad de combate de un oponente.

Palabras clave: Guerra de la Información – Teatro de Operaciones – Tecnología de la información.

Introducción

Distintos intereses como los económicos, tecnológicos y la defensa, entre otros, movilizan a los Estados, empresas, organizaciones armadas y otras a pujar por obtener información utilizándola para beneficios propios y en detrimento de un oponente o competidor.

Esta puja dentro del ámbito militar, al cual nos vamos a referir, se define como Guerra de la información (GI) o InformationWar (IW) abarcando entre otros aspectos, lo que conocemos como C4I (Comando, Control, Comunicaciones, Computación e Inteligencia).

Es muy probable que estetipo de Guerra domine el espectro de los conflictos del siglo XXI, ya que el hecho de lograr el dominio de información sobre el adversario ha adquirido una relevancia especial, pudiendo tal vez, hasta dirimir conflictos mucho antes del empleo de otras formas violentas de resolverlos.

En 1991, el profesor de la Universidad Hebrea de Jerusalén Martín Van Creveld publicó un libro titulado "La Transformación de la Guerra", que aportaría sustento intelectual a la teoría de la Guerra de cuarta generación. El autor sostiene que la guerra ha evolucionado hasta un punto en que la teoría de Clausewitz resulta inaplicable.

Van Creveld prevé que en el futuro las bases militares serán remplazadas por escondites y depósitos, y el control de la población se efectuará mediante una mezcla de propaganda y terror.

Además afirma que las fuerzas regulares se irán trasformando en algo diferente a lo que han sido tradicionalmente. También prevé la desaparición de los principales sistemas de combate convencionales y su conversión en conflictos de baja intensidad (también llamados Guerras Asimétricas).

En las últimas tres décadas el avance de las computadoras y el desarrollo de las redes de interconexión alcanzado primeramente entre ellas en forma local y posteriormente formando la madre de todas la redes, la internet, ha dado a cada individuo la posibilidad de acceder a información que antes tenía vedada.

Adams James en su libro “La próxima Guerra mundial” señala que “La revolución del ordenador ha dado lugar a la aparición de un mundo diferente. Este será un lugar donde las guerras de todo tipo no serán libradas por soldados contra soldados, sino por nuevos guerreros de la infoesfera. En este mundo nuevo el soldado será, capaz de

plantar un virus en cualquier red.[1]

Ante la posibilidad certera de acceso a datos por parte de individuos a través de internet y otros medios, pensemos entonces la capacidad que puede alcanzar y obtener un Estado u organizaciones adiestradas con métodos y medios tecnológicamente aptos que incrementen sus posibilidades de acceder a la información que necesitan.

El dominio, uso y manejo de la información es lo que determina esta nueva forma de combate conocida como GI, si bien como una técnica independiente de hacer la guerra, no existe, la misma está compuesta por varias piezas que la conforman. Estas piezas comprenden la protección, la manipulación, la degradación y la denegación de información

Tal vez la definición de GI más ampliamente aceptada por las Fuerzas Armadas mundiales, es la del Departamento de Defensa de los Estados Unidos: "La Guerra de la Información son acciones llevadas a cabo para el logro de la superioridad de la información, afectando la información, los procesos basados en la información y los sistemas de información adversarios, mientras se protege la información, los procesos basados en la información y los sistemas de información propios".[2]

Es por ello que el dominio de la información en el campo operacional es fundamental ya que alcanzarlo, permite por un lado tener un panorama completo de todo lo que sucede en el campo de batalla y por otro cerrarle al oponente el acceso a todas sus posibles fuentes de información.

No obstante, poco interés se ha puesto en referirse específicamente a la Guerra de Información dentro de un Teatro de Operaciones, de aquí que formulamos los siguientes interrogantes:¿Qué influencia tendrá la Guerra de la Información dentro de un Teatro de Operaciones?, ¿Puede ésta vencer un oponente sin un enfrentamiento armado?

En correspondencia con los interrogantes formulados se plantean los siguientes objetivos: determinar la influencia que la Guerra de la Información tiene dentro de un Teatro Operaciones, de qué manera esta nueva forma de combate puede cambiar el desarrollo de las operaciones influyendo directamente en la toma de decisiones de un

[1]James, Adams: La próxima guerra mundial, pp.15-16, Granica, Buenos Aires , 1996.

[2]Reto, Haeni. E. Information Warfare: The George Washington University Cyberspace Policy Institute 2033 K Str. Suite 340 N Washington DC 20006

Comandante de teatro y como la GI puede deteriorar la capacidad y voluntad de combate de un oponente antes del comienzo de las hostilidades.

En tanto la hipótesis que guíael trabajo afirma que: Contar con un eficiente sistema abocado al desarrollo ofensivo y defensivo de GI dará a quien lo posea ventaja sobre su oponente.

El alcance de este escrito está orientado a revelar cómo el uso de la tecnología en un Teatro de Operaciones está marcando la tendencia en los nuevos conflictos que buscan ser resueltos en un corto periodo de tiempo y con el menor número de víctimas posibles en ambos bandos.

Para una mejor comprensión de los contenidos que aquí se desarrollan, el trabajo se estructura en dos capítulos. En el primer capítulo se podrá apreciar como con el correr del tiempo, las confrontaciones bélicas y los avances tecnológicos han evolucionado y se ha dado preponderancia a la utilización de la información en el uso de operaciones militares. En el segundo capítulo se definen los ámbitos donde esos avancen se aplican y como pueden afectar las operaciones de Guerra de la Información, además veremos como la aplicación de métodos de planificación actuales son compatibles con esta nueva forma de realizar operaciones militares.

Capítulo I: Evolución de la guerra de la información

"La información es la moneda de la victoria en el campo de batalla"

General Gordon R. Sullivan[3]

Los desarrollos tecnológicos alcanzados durante los últimos años han facilitado la forma de obtener y proteger la información vital para una nación. Durante una contienda armada la necesidad de contar en tiempo y forma con información sobre el oponente se implementa desde el comienzo de las guerras pero podemos decir, que el auge de esta necesidad de obtención de datos sobre el adversario, llegó a su plenitud durante la conocida Guerra Fría.

En ella las dos principales potencias mundiales (EE.UU – URSS) y sus aliados pugnaban por obtener uno, secretos del otro aplicando todos los métodos conocidos para este fin realizando además novedosos desarrollos tecnológicos para lograrlo, frecuentemente con fines propagandísticos, para presentar al mundo éxitos tecnológicos inéditos y espectaculares. De allí habría nacido el afán de apropiarse de investigaciones científicas de la contraparte, que permitiría exhibir resultados con mayor rapidez y a menor costo.

En las últimas décadas, el avance de las computadoras y el desarrollo de las redes de interconexión alcanzado primeramente entre ellas en forma local y posteriormente formando la madre de todas la redes, la internet, ha eliminando las barreras geográficas dando a cada individuo la posibilidad de acceder a información que antes tenía vedada.

La información brindada por la Unión Internacional de Telecomunicaciones (UIT) y utilizados por la ONU afirman que:

"Al final del año 1997, sólo el 1,7% de la población mundial, 70 millones de personas, había utilizado la Internet. En el año 2009, el número de usuarios aumentó aproximadamente
a 1.900 millones de personas que representan el 26% de la población mundial".[4]

[3] Sullivan, Gordon R., General (R) del Ejercito de EE.UU nació en Boston, Massachusetts, el 25 de septiembre de 1937.

[4]ONU: XII Congreso de Naciones Unidas sobre «Prevención del delito y justicia penal», «La falta de cooperación internacional facilita una vía de escape a los delincuentes cibernéticos.» Salvador (Brasil), 12

Año a año se ha venido registrando un sostenido crecimiento de usuarios de Internet "en el año 2006 el número de usuarios de Internet fue de 1.100 millones, previéndose para el año 2016 que el número ascenderá a 2.000 millones"[5], este incremento trae aparejado por ende una mayor vulnerabilidad de las redes de las Fuerzas Armadas ha ataques cibernéticos, por lo cual: "Es innegable que las guerras del siglo XXI serán diferentes de las que caracterizaron al siglo XX"[6]

Gráfico N° 1: Evolución mundial del uso de internet[7].

El creciente incremento de personas que a través de sus computadoras se conectan entre sí por medio de las distintas redes globales, ha producido un aumento en las amenazas, en las vulnerabilidades, en los riesgos y en los ataques sufridos por los consumidores (robo de claves, identidades, tarjetas de crédito, etc)

Si individuos en algún lugar del mundo desde su hogar u oficina tienen la posibilidad de acceso a datos de otras personas en forma clandestina, pensemos

---

a 19 de abril de 2010, en: *http://www.un.org/es/events/crimecongress2010/pdf/factsheet_ebook_es.pdf*. consultado agosto 2012.

[5]"Hay 16 millones de usuarios de Internet en la Argentina", Infobae.com consultado 15 de abril de 2010, en: http://www.infobae.com/tecnologia/353634-100918-0-Hay-16-millones-usuarios-internet-la-Argentina

[6]Schmitt, Michael: La guerra de la información: los ataques por vía informática y el jus in bello, Comité Internacional de la Cruz Roja, 2002, Disponible en: http://www.icrc.org/web/spa/sitespa0.nsf/html/5TECG3 consultado 13 de junio de 2011.

[7]Emprende Mundo. Disponible en : http://emprende-el-mundo.blogspot.com.ar/2009/06/comercio-electronico-entrevista-con.html consultada septiembre 2012

entonces la capacidad que pueda tener una nación o grupo organizado bien adiestrado con métodos y medios tecnológicamente aptos que incrementen la capacidad de acceder a información vital.

Esta nueva realidad surgida en las últimas dos décadas, desplazó a los medios de inteligencia tradicionales como recurso para obtener información de un oponente, lo cual llevó al surgimiento de nuevas fortalezas y debilidades de los actores presentes en un escenario de conflicto armado donde el débil, no es quien no logre desarrollos tecnológicos de última generación, sino que será más bien el que se nutrirá de los que en general ya están disponibles en el mercado global y que no necesariamente son de exclusivo uso militar: Esto provoca enfoques diferentes ante una misma realidad:

"La revolución del ordenador a dado lugar a la aparición de un mundo diferente. Este será un lugar donde las guerras de todo tipo no serán libradas por soldados contra soldados, sino por nuevos guerreros de la infoesfera En este mundo nuevo el soldado será, capaz de plantar un virus[8] en cualquier red[9]".

Es en este sentido que distintos intereses como los económicos, tecnológicos y de defensa, entre otros, movilizan a los Estados, empresas, organizaciones armadas y otras a pujar por obtener información utilizándola para beneficios propios y en detrimento del oponente o competidor. Esta disputa a la que nos referiremos en el ámbito militar es la llamada Guerra de la información (GI) o InformationWar (IW) abarcando entre otros aspectos el C4I (Comando, Control, Comunicaciones, Computación e Inteligencia).

Es muy probable que este tipo de guerra domine el espectro de los conflictos del siglo XXI, ya que el hecho de lograr el dominio de información sobre el adversario ha adquirido una relevancia especial, surgiendo el interrogante si esta nueva forma de guerra podrá dirimir conflictos mucho antes del empleo de otras formas violentas y devastadoras de resolverlos.

En distintos ámbitos internacionales relacionados a la defensa han denominado a la GI de diferentes formas, según el InstituteforNational Security Studies-US Air Force Academy: "La Guerra de la información se centra en la gestión y el uso de la

[8]Virus informático: programa que tiene por objeto alterar el normal funcionamiento de los ordenadores, sin el permiso o el conocimiento del usuario; habitualmente reemplazan archivos ejecutables por otros infectados.

[9]James, Adams: La próxima guerra mundial, pp.15-16, editorial Granica, Buenos Aires (Argentina), 1996.

información, en todas sus formas y niveles, para lograr una ventaja militar decisiva.[10]

La Naval Posgraduate School define a la guerra de información como: "Cualquier forma de interferir o impedir el acceso a la información, con el objetivo de causar en el usuario la toma de decisiones erróneas, para confundir o colapsar sus comunicaciones o la toma de decisiones".[11]

En la Argentina, el Estado MayorGeneral de las Fuerzas Armadas define a la guerra de la información como "El uso y manejo de la información con el objetivo de conseguir una ventaja competitiva sobre un oponente, pudiendo consistir en la recolección de información táctica, en la confirmación de la veracidad de la información propia, en la distribución de propaganda o desinformación a efectos de desmoralizar al enemigo, socavar la calidad de la información de la fuerza enemiga y negarle las oportunidades de recolección de información, pudiendo adquirir diversas formas"[12].

Basándonos en estos conceptos es que el dominio de la información en el campo operacional es fundamental; ya que alcanzarlopermite por un lado tener un panorama completo de todo lo que sucede en el campo de batalla y por otro cerrarle al oponente el acceso a todas sus posibles fuentes de información, además de influir directamente no solo en las fuerzas empeñadas en combate sino en todos los integrantes de la nación oponente.

En este sentido podemos decir que a fines de la década del 60, la guerra de Vietnam fue la primera guerra transmitida por televisión, si bien era vista en forma diferida (luego de varias horas de haber ocurrido los hechos) los ciudadanos norteamericanos tenían acceso a ver que ocurría con sus tropas al otro lado del mundo como si fuera un programa diario.

Fue en enero del 1968 en Vietnam del sur, mientras se festejaba el año nuevo denominado en esta cultura como Tet, ocurrió un contraataque conjunto entre el Ejército de Vietnam del Norte y el Vietcong conocido como la ofensiva del Tet. En esta operación, los vietnamitas tomaron las principales ciudades y poblados llegando a ocupar hasta le mismo Shanghái (Vietnam del Sur) dejando a su paso a miles de

[10]Aldrich, Richard W.: The international legal implications of information warfare, Colorado (EstadosUnidos), Information Warfare Series, USAF Institute for National Security Studies US Air Force Academy, 1996.

[11]Thrasher, Dean Roger: Information warfare Delphi: raw results, p. 4, Monterey, 1996.

[12]Estado Mayor Combinado: PC 00-02 Glosario de términos de empleo militar para la acción militar conjunta. Proyecto, 2010.

Norteamericanos muertos a la vista de millones de televidentes estadounidenses que veían azorados las imágenes en la comodidad de sus hogares.

Luego de reiteradas manifestaciones de victoria hechas por el poder político días antes a este hecho, chocar a través de un televisor con la realidad de una ciudad totalmente sitiada con miles de sus compatriotas asesinados tirados en medio de las calles de una ciudad a miles de kilómetros, causó un caos interno y dividió a la sociedad.

El acceso que tuvo la ciudadanía a esta información y que el gobierno no pudo controlar influyó de manera letal en la imagen del gobierno de LyndonBaines Johnson, generando un gran rechazo a la contienda por parte del pueblo estadounidense.

Dos décadas después, la primera guerra del Golfo en 1991 fue la primera guerra televisada del mundo pero esta vez prácticamente en vivo y en directodonde podíamos observar los enfrentamientos cuando estaban ocurriendo sumando además un shock psicológico al ver pequeñas siluetas de soldados Iraquíes en movimiento, sucumbir sin ningún tipo de posibilidad de supervivencia ante las armas norteamericanas.

La difusión de estas imágenes entre otras acciones psicológicas transmitidas en forma masiva por parte de los canales televisivos, radios y todos los medios de comunicación permitieron a los EE.UU quebrar la voluntad de lucha de la mayoría de los soldados del régimen de Saddam Hussein y, contrariamente a este aspecto, implantó una sensación de indestructibilidad en los soldados norteamericanos, mejorando su moral, el cumplimiento de órdenes y el espíritu de lucha.

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

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

Las potencias mundiales encabezadas por Alemaniaestán buscando desarrollar en forma combinada una doctrina rectora en este tipo de actividades, para integrarla en el área de misiones combinadas dentro del ámbito militar. La operación se llama el "Experimento de Operaciones de la Información Multinacional"[13] ("MNIOE" en inglés).

Los participantes actuales de este proyecto definen a las Operaciones de la Información como "El suministro y coordinación de las actividades militares que afectan a la información y a los sistemas de información, incluyendo el comportamiento del sistema y sus capacidad para crear los resultados deseados."

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

No podemos dejar de mencionar el nuevo ámbito donde se desarrollaran la mayoría de las batallas en la GI, el Ciberespacio. Este término fue utilizado por primera vez por William Gibson, escritor norteamericano en su novela de ciencia ficción: *Neuromante* publicada en el año 1984[14] y en términos generales se refiere a una realidad virtual donde se agrupan usuarios, páginas *web*, *chats*, servicios de Internet y otras redes.

En este nuevo ámbito de interacción, una de las principales vulnerabilidades es la afectación de infraestructuras críticas la cual se logra a través de: "Herramientas y procedimientos para realizar ataques a redes que pueden obtenerse fácilmente, en Internet. El ciberespacio ofrece el medio para realizar ataques organizados a distancia, solamente es necesario disponer de la tecnología necesaria, además, permite a los atacantes esconder sus identidades, localizaciones y rutas de entrada"[15].

Relacionado a la tipificación de infraestructuras críticas de información y ciberseguridad, la República Argentina ha definido que: "La utilización de las comunicaciones virtuales es un recurso que depende de la infraestructura digital, la cual

[13]Multinational Information Operations Experiment - Disponible en: http://www.mnioe.info/index.php?id=12 consultada agosto 2012

[14]Diccionario de Informática: en: *http://www.alegsa.com.ar/Dic/ciberespacio.php* , consultado 10 de julio de 2011.

[15]Puime Maroto, Juan: «La violencia del siglo XXI. Nuevas dimensiones de la guerra», en «El ciberespionaje y la ciberseguridad», p. 51, CESEDEN, Ministerio de Defensa, Madrid, 2009.

es considerada como infraestructura crítica, entendiéndose ésta como imprescindible para el funcionamiento de los Sistemas de Información y Comunicaciones, de los que a su vez dependen de modo inexorable, tanto el Sector Público Nacional como el sector privado, para cumplir sus funciones y alcanzar sus objetivos".[16]

Cuando hablamos de operaciones en el ciberespacio debemos tener en cuenta que si bien las acciones se originan en computadoras *(hardware)* que tienen un componente físico, estas se realizan a través de una realidad no asible materialmente, afectando finalmente algo material del enemigo.

Podemos decir entonces que las "operaciones de información" son el empleo integral de la guerra electrónica, las operaciones psicológicas, el engaño militar y las operaciones de seguridad, en conjunto con capacidades especificas de apoyo, para influenciar, interrumpir, corromper o usurpar las decisiones de los adversarios humanos y automatizados para proteger las propias. En este sentido, si se posee una mayor capacidad tecnológica se tendrá una ventaja militar la cual proporcionará una fuerza superior en ese nivel de la guerra.

Simultáneamente requerirá negarle al adversario la oportunidad de actuar contra las propias vulnerabilidades estratégicas; principalmente debido a la creciente dependencia de la transmisión de datos sobre las infraestructuras críticas de información y ciberseguridad en forma digital por las redes electrónicas.

Otro aspecto de la guerra de la información que cumple un rol fundamental en estas batallas son los medios de comunicación social (MM.CC.SS), que pueden influir en forma directa en la voluntad y el estado de ánimo de una nación cambiando así el rumbo de una contienda.

Para ello el Departamento de Defensa de EE.UU formó una sociedad con la hasta entonces poco conocida a nivel mundial cadena de noticias CNN, logrando así demostrar que esta disputa era justa y justificada para la libertad y por el bien de la humanidad[17].

EE.UU finalmente liberó Kuwait, hecho transmitido en vivo y en directo por CNN, quedando en la mente del mundo como una guerra de ultra tecnología y el gran valor de las tropas norteamericanas, gracias a la propaganda llevada a cabo.

---

[16]Jefatura del Gabinete de Ministros: resolución 580/2011. Créase el Programa Nacional deInfraestructuras Críticas de Información y Ciberseguridad, Bs. As., 28 de junio de 2011.

[17]Narváez Rosero, Edison: Guerra Psicológica en http://www.fuerzasarmadasecuador.org/informacion-variada/guerra-psicologica/ consultada septiembre de 2012

Capítulo II: Ámbitos para llevar a cabo la guerra de la información.

Durante las dos últimas décadas, se ha producido un boom tecnológico, y con esas tecnologías se generaron cambios radicales en la naturaleza de los sistemas militares. Los medios espaciales de reconocimiento y vigilancia, los vehículos aéreos no tripulados y cientos de sistemas de sensores terrestres condujeron al desarrollo de capacidades de Inteligencia, Vigilancia y Reconocimiento (IVR) que no hubieran podido imaginarse unas décadas atrás.

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

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

De la misma forma que estos sofisticados medios brindan una fortaleza para quien los posee también sin duda, son una gran debilidad. Esto quedó demostrado cuando un equipo de la Universidad de Texas logró hackear un avión no tripulado de última generación (RQ-170) usando equipos y componentes del mercado civil invirtiendo solamente 1000 dólares. Esta operación se realizó en coordinación con el Departamento de Seguridad Nacional de EE.UU con la idea de demostrar que el esquema actual de comunicaciones que sirven para guiar y controlar estos aviones es vulnerable según explica el sitio de la BBC[18].

Si bien estos medios son una de las principales formas para que un Comandante reciba información, esta irá evolucionando en forma constante ya que frente a él se encuentra otro ser pensante con las misma necesidades pero con intereses opuestos que tratará por todo los medios impedir que cumpla sus objetivos y, por tal motivo, intentará transferir la incertidumbre y negar el conocimiento a su oponente.

La guerra de la información, no es sólo un tipo de guerra en sí misma, sino que está formada por un conjunto de actividades.Es por ello que tal vez un Comandante sólo

[18]BBC Mundo. Disponible en: http://www.bbc.co.uk/mundo/noticias/2012/06/120629_avion_notripulado_hackers_gps_en.shtmlconsultado en agosto de 2012

necesite utilizar alguno de esos subcomponentes que la conforman de acuerdo a sus necesidades o en todo caso darle más preponderancia a uno que otro, esto estará determinado por el enemigo al que enfrente o los efectos que busque causar sobre éste. También permitirá al Comandante operar dentro del "Circuito OODA" (observar – orientar - decidir -actuar) en todos los niveles del conflicto, desde el táctico hasta el estratégico.

1.2 Principios de la guerra de la información.

En una publicación realizada por el sitio web de AFCEA Argentina, el Capitán de Navío Jorge Minoletti Olivares hizo mención a los ocho principios para llevar adelante la guerra de la información, estos son:

Decapitación: Este principio establece que el comando y control, los sistemas de apoyo a la toma de decisiones y las comunicaciones debieran ser el principal objetivo de la Guerra de Información de modo de aislar al comando adversario de sus fuerzas de combate.

Prioridad de Sensores: Este principio establece que todos los sensores enemigos deben ser suprimidos o destruidos antes de entrar en combate.

Conocimiento: El principio del conocimiento indica que debe estar disponible tanta información como sea posible para aquellos que la necesitan y que su distribución debe ser lo más fluida como se pueda. En otras palabras, establece que la información de inteligencia debe dejar de ser enviada a un mando central para su posterior distribución. Esta es una medida defensiva y no ofensiva como se pretende.

Volatilidad: Este principio establece que debe haber una estrecha relación entre el sentido de urgencia y el proceso de toma de decisiones. Esto reconoce lo efímero de la naturaleza de la información.

Supervivencia: La política y la estrategia deben ser centralizadas, pero la planificación y la ejecución deben ser descentralizadas, para dificultar tanto como sea posible, un ataque del enemigo. En otras palabras, todos deben tener claro el panorama general para estar en las mejores condiciones de contribuir al logro de los objetivos cuando el mando central se vea afectado en su sistema de comando y control. En vez de operar con una estructura jerárquica tradicional, se debe actuar en un ambiente de red.

Interoperatibilidad: Los sistemas de comunicaciones y de almacenamiento de información deben ser lo más interoperables posible de modo de compartir al máximo la información disponible. Muchas veces la tecnología actual impide traspasar información

vital por problemas de compatibilidad de equipos de comunicaciones. Por ejemplo, un controlador aéreo adelantado de la Fuerza Aérea debiera estar en condiciones de comunicarse con el piloto de una aeronave de la Aviación Naval que lo sobrevuele, en vez de tener que seguir toda la cadena de mando a través de los centros de la Armada y de la Fuerza Aérea.

Jerarquía: Este principio indica que se deberá aplicar en contra del adversario, toda la tecnología disponible para llevar a cabo una Guerra de Información, aunque parezca que el enemigo no es capaz de desarrollar este tipo de guerra.

Intensidad: Se deberá desarrollar todo el esfuerzo posible y se deberá evitar interferencias políticas en el nivel operacional. Restricciones en este sentido representan vulnerabilidades que pueden ser explotadas por adversarios internos o externos.

2.2 Operaciones de Guerra de Información.

Al igual que en el resto de las operaciones militares y en las doctrinas de las distintas fuerzas armadas del mundo existen entre otras, dos tipos de operaciones las ofensivas y las defensivas. Las operaciones ofensivas tienen como única finalidad negar el uso de la información necesaria para la toma decisiones al Comandante enemigo, por el contrario las defensivas son aquellas por las cuales debemos evitar que el Comandante enemigo despeje sus incertidumbres antes, durante y después de las operaciones afectando la conducción de nuestras operaciones.

Entre los ámbitos donde se pueden llevar adelante las operaciones de información que abarcan la protección, la manipulación, la degradación y la denegación de información podemos distinguir:

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

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

Para evitar esto los elementos y órganos de comando, operativos, logísticos y servicios de apoyo, necesarios para cumplir cualquier misión militar que forman un conjunto variado y complejo deben estar interrelacionados, de modo que cada uno de los diferentes escalones y elementos pueda disponer de la información necesaria en cada momento y a la vez enviar sus órdenes, requerimientos o información a los otros elementos es por ello que para poder cumplir con la misión impuesta, esto debe hacerse con precisión y en oportunidad.

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

Si le sumamos al comando y control, las comunicaciones, la inteligencia y la informática formamos lo que se conoce como C4I, en su conjunto, estos sistemas entregan a los Comandantes una visón acabada del campo de batalla, incluyendo terreno y clima, dispositivo de las fuerzas propias (tamaño, ubicación, dirección de empleo, estado operacional, logística) y dispositivo del enemigo con idéntico detalle.

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

Estos cambios, a su vez, deben ser observados, evaluados por los receptores y actuar en consecuencia generando así un proceso continuo, este proceso puede ser pensado como un "ciclo de decisión" es por ello que las operaciones sobre el Comando y Control del enemigo tiene como finalidad anular, influenciar, perturbar o retrasar este ciclo de decisión, pudiendo invalidar de esta manera el desarrollo de las operaciones. De aquí entonces la importancia vital de proteger el sistema de cualquier agresión o interferencia a este sistema que podría cancelar el empleo de las FF.AA con la anulación o interferencia del propio C4I.

En relación con estas tecnologías, los EE.UU diseñaron la estructura C4 ISR (Comando, Control, Comunicaciones, Computación, Inteligencia, Seguridad y

Reconocimiento) en su Visión Conjunta 2010, que provee ventajas de procesamiento de información y comunicación a través de una red de sensores que permite un conocimiento del campo de batalla en tiempo real hasta un espacio de 300 km.[19]

Ciberguerra: El uso de ciberespacio por Fuerzas Armadas, como nuevo ámbito en las guerras del siglo XXI, impondrá cambios para optimizar su empleo en forma disuasiva o efectiva para enfrentar agresiones que provengan de el, podríamos diferenciar dos tipos de actores que pueden emplear el ciberespacio con fines no pacíficos, según sea su naturaleza: Delincuentes, Fuerzas Armadas.

La Ley de Defensa Nacional de la República Argentina (Ley 23.554) determina que la Defensa Nacional: "Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes"[20]

Definiremos entonces como ciberguerra a "toda agresión externa de Fuerzas Armadas de un Estado, que utilizando el ciberespacio, ataque los sistemas de decisión y gestión, infraestructura y/o sistema de defensa, afectando la capacidad de garantizar de modo permanente la soberanía e independencia, integridad territorial y capacidad de autodeterminación de otro actor, así como proteger la vida y la libertad de sus habitantes".

Esta nueva forma de agresión se lleva a cabo mediante la transmisión de virus[21] para realizar un ataque a las redes a menudo proviene de ordenadores zombis [22], quedando los verdaderos atacantes fuera de alcance ocultos tras dejar rastros falsos.

El presidente de los Estado Unidos Barack Obama declaró en el año 2010 que: "El crecimiento y la expansión de la tecnología ya ha transformado la Seguridad Internacional y el mercado global. Mientras Estados Unidos, la nación que creó la

[19] http://www.afcea.org.ar/publicaciones/conciencia.htm consultada en agosto de 2012

[20] http://www.mindef.gov.ar/publicaciones/derechos_humanos/Ley-de-Defensa-Nacional.phpconsultado 10 de mayo de 2012.

[21] Virus informático: programa que tiene por objeto alterar el normal funcionamiento de los ordenadores, sin el permiso o el conocimiento del usuario; habitualmente reemplazan archivos ejecutables por otros infectados.

[22] Denominación que se asigna a ordenadores personales que tras haber sido infectados por algún tipo de virus, pueden ser usadas para ejecutar actividades hostiles, sin la autorización o el conocimiento del usuario del equipo, en: http://www.adn.es/tecnologia/20080818/NWS-1038-ordenador-zombie-infectado-spam.htmlconsultado 15 de abril de 2012.

Internet y lanzó una revolución informática, continúe siendo pionero tanto en la innovación tecnológica como en la seguridad cibernética, mantendremos nuestro poderío, capacidad de recuperación y liderazgo en el siglo XXI".[23]

Como ejemplo de un ataque informático tomaremos lo ocurrido en Estonia en el año 2007, el 9 de mayo se festeja en Rusia el día de la Victoria conmemorando el día que ejército Ruso venció al ejército Alemán .El 15 de abril de 2007 el gobierno de Estonia, decido remover el monumento que homenajeaba a los caídos en esta fecha, recibiendo distintas amenazas en caso de concretar este hecho entre ellas un ataque cibernético.

El 26 de abril de ese año por la noche un ataque cibernético comenzó inutilizando todas la paginas gubernamentales y las de los partidos políticos, días más tarde todos los MM.CC.SS quedaron totalmente bloqueados para transmitir, días después otro ataque logro desconectar todo el sistema financiero y bancario dejando hasta los cajeros automáticos fuera de servicio. El gobierno de Estonia acuso por estos hechos al Gobierno Ruso pero este siempre lo negó.

Los ataques surgieron de todo el mundo, pero los funcionarios de Estonia y los expertos en seguridad informática señalan que, especialmente durante la fase inicial, se identificó a algunos atacantes por sus direcciones de Internet, muchos de los cuales eran rusos, y algunos miembros de instituciones estatales rusas.[24]

Otro caso trascendente de espionaje cibernético desarrollado por el Centro Superior de Estudios para la Defensa Nacional dependiente del Ministerio de Defensa Español[25] explica que el mismo ocurrió en el año 2008, en este acto el ataque se produjo sobre las redes clasificadas de las computadoras militares del departamento de Defensa de los Estados Unidos (DoD)estas se vieron significativamente comprometidas. El ataque comenzó cuando una unidad flash (Pen Drive)infectada fue introducida en una computadora portátil (laptop)en una base en el Oriente Medio.

El código de la computadora maliciosa de la unidad flash, colocado ahí por una Agencia de Inteligencia extranjera, se auto cargó a una red administrada por el Comando Central de Estados Unidos. Ese código se esparció sin ser detectado en los

[23]Ágora revista disponible en:
http://agorarevista.com/es/articles/rmim/features/homeland-defense/2011/04/01/feature-01 consultado 16 de septiembre de 2012.

[24]Piratas Informáticos abren fuego en el ciberespacio, volumen 3, p. 41, Estados Unidos, 2010.

[25] Los ámbitos no terrestres en la guerra futura: Espacio - CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL – Monografías del CESDEN – Editado por el Ministerio de Defensa Español – mayo 2012

sistemas clasificados y no clasificados, estableciendo lo que equivale a un puesto de avanzada digital, del cual se podían transferir datos a servidores bajo control extranjero.

El peor temor de un administrador de redes un programa paria funcionando silenciosamente, listo para entregar planes operacionales en las manos de un adversario desconocido.Este incidente fue la ruptura más significativa a la seguridad en las redes militares de Estados Unidos conocida hasta ahora y sirvió como una alerta importante. La operación del Pentágono para contrarrestar este ataque se llamo BuckshotYankee, este hecho marco un momento decisivo para la estrategia de ciberdefensa de Estados Unidos[26]

En el año 2009 EE.UU estableció un Comando Cibernético, organizado bajo su Comando Estratégico, el cual inició sus operaciones en mayo del 2010 en Fort Meade (Maryland) su primer comandante, el general Alexander, explicó los objetivos del mismo: "USCYBERCOM tiene la responsabilidad de dirigir las operaciones y la defensa diaria de las redes informáticas del DoD; planificar, integrar y sincronizar las actividades cibernéticas en forma sistémica y cuando así se ordene bajo la autoridad del presidente, del secretario de Defensa y del Comandante del Comando Estratégico de Estados Unidos de América, conducir operaciones militares cibernéticas de espectro total para asegurar la libertad de acción de Estados Unidos de América y los aliados en el ciberespacio. USCYBERCOM centraliza el mando de las operaciones militares ciberespaciales, fortalece las capacidades ciberespaciales del DoD e integra y aumenta la experiencia cibernética del mismo"[27]

En septiembre del 2010 se produjo lo que se conoció como el primer caso conocido de virus que intentó causar un daño significativo en una planta nuclear. El virus nombrado como *stuxnet*, infectó alguno de los sistemas de control de la central nuclear iraní de Bushehr, especialmente el Sistema de Control de las centrifugadoras (de aluminio), provocando que comenzaran a girar un 40% más rápido durante un breve período de tiempo (aproximadamente 15 minutos) y causando grietas en ellas; otra

[26]Lynn II, William J.: «Defendiendo un nuevo ámbito. La ciberestrategia del Pentágono», Manual de Informaciones, volumen LIII, p. 33, Buenos Aires, junio-agosto de 2011

[27]Keith B, Alexander : «El dominio de los guerreros cibernéticos», MilitaryInforma-tionTechnology,volumen 4, número 2, Agence France-Presse, 2011.

función del virus había sido grabada en el *software* del equipo, como un registro, y su función fue evitar que la alarma del equipo se activara y alertara a los operadores.[28]

Este acto demostró que se puede poner en peligro instalaciones vitales de una nación, demostrando que de la misma manera se puede afectar el control de todo tipo de armas así como su sistema de guiado sin ser detectados por los usuarios.

No podemos dejar de mencionar en este ámbito a los soldados informáticos, aquellos quienes sin mediar edad, raza, religión o convicciones políticas y sentados desde la comodidad de su casa u oficina ofician de nuevos guerreros del ciberespacio conocidos como "hackers".

Acción Psicológica: Son las operaciones de información que se utilizan para lograr una modificación en las conductas y mentes de las personas buscando aceptación y adaptación a las ideas que se tratan de imponer por medios pacíficos. Los objetivos que persigue esta tipo de operaciones aplicadas en el ámbito militar, van desde quebrar la voluntad de lucha de las FF.AA opositoras hasta generar una aceptación grata y sumisa a las fuerzas invasores por parte de la población local, logrando transformar a sus propios gobernante en los enemigos de la ciudadanía.

Existiendo también las operaciones dentro de las propias FF.AA buscando mantener la moral interna alta y el espíritu de lucha. Uno de los ejemplos históricos más conocidos de acción psicológica realizados en una contienda se realizo durante la segunda guerra mundial, en la batalla del pacifico por las fuerzas japonesas las cuales pergeñaron un plan para afectar el espíritu de lucha norteamericano.

El mismo consistió en crear una figura radial conocida como la Rosa de Tokio[29], el papel era representado por una mujer de voz dulce y tierna que durante muchas horas en las noche leía supuestas cartas que habían sido capturadas por las fuerzas japonesas y en un acto de generosidad el gobierno japonés se las hacía llegar a través de la radio.

Las misivas eran redactadas por especialistas con un destinatario exclusivo, un nombre al azar, solo un nombre que se descartaba que ese nombre era portado por varios combatientes quienes se iban a sentir identificados, las cartas referían a los

[28] Los ámbitos no terrestres en la guerra futura: Espacio - CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL – Monografías del CESDEN – Editado por el Ministerio de Defensa Español – mayo 2012

[29]Clarin. com.Disponible en:

http://edant.clarin.com/diario/2006/09/28/elmundo/i-02501.htm consultada septiembre 2012

sentimientos de esposas, hijos, novias, padres y madres quienes les pedían que dejaran de pelear y volvieran a casa, también referían a la muerte de un ser querido, el poco apoyo nacional a la guerra y cientos de causas más que solo buscaban quebrar moralmente a los soldados norteamericanos.

Años mas tarde a comienzos de este siglo, en octubre del 2002 comenzó la Segunda Guerra del Golfo, conocida también como operación "LIBERTAD DURADERA", así denominada por los propagandistas del Pentágono norteamericano. Al inicio de las operaciones militares la enorme infraestructura de propaganda aliada ya estaba montada y millones de hojas volantes inundaban la parte meridional de Iraq buscando entrar en el inconsciente de la población civil y soldados iraquíes, neutralizando su voluntad de resistir a las tropas aliadas, incitando a que no se destruya la infraestructura petrolera y persuadiéndola de no apoyar a Hussein[30].

En contra parte de esto la operación que se realizo puertas adentro de las propias FF.AA tenía como objetivo de la acción psicológica, crear la conciencia de una guerra rápida y con un costo de heridos y muertos norteamericanos mínimo; hacia fuera se quería construir la imagen de una fuerza "libertadora" y no invasora, que evitaba al máximo la muerte de población civil y el daño a la infraestructura que no fuese gubernamental.

Estos casos nos muestran la necesidad que un comandante operacional cuente con plan de operaciones psicológicas, este plan bien concebido y llevado a cabo por expertos podrá marcar la diferencia en la voluntad de lucha propia y la del oponente.

Inteligencia: Desde el principio de los conflictos armados existe dentro de las operaciones militares una en especial y sin duda la precursora de obtención de información, encargada de recolectardatos acerca del enemigo actual o potencial. Esta información recolectada nos permitirá a futuro nutrir a un comandante con los datos necesarios para que logre planear en forma adecuada las operaciones.

La inteligencia militar basa su esfuerzo de obtención en lograr adquirir información respecto a la capacidad tecnológica, el orden de batalla enemigos, capacidad de transporte y vías de comunicación, etc. Estos datos le permitirán a un comandante de teatro poder emplear eficazmente sus medios sobre el oponente.

[30]Narváez Rosero, Edison: Guerra Psicológica disponible en: http://www.fuerzasarmadasecuador.org/informacion-variada/guerra-psicologica/

Así como la obtención de información es vital para las operaciones también lo es la negación de la misma información propia al oponente, para ello la inteligencia complemente su etapa de producción con la de negación de información denominada contrainteligencia destinada a negar a un adversario presente o futuro obtener información vital que pueda afectar los propios intereses.

Engaño militar: Se define como las acciones realizadas de forma deliberada para inducir a un error al adversario tanto en sus capacidades militares, intenciones y operaciones, lo que provoca a este tomar acciones equivocadas que contribuyan al cumplimiento de la misión propia.

Las operaciones militares de engaño son un poderoso instrumento militar, depende de la inteligencia identificaren forma apropiada los objetivos a ser engañados. La Doctrina de Operaciones Conjuntas de EE.UU. define el engaño como: "Las medidas destinadas a engañar al enemigo mediante la manipulación, distorsión o falsificación de pruebas para inducirle a reaccionar de manera perjudicial para sus intereses"[31].

Estos métodos de GI son aplicables en todos los niveles de la guerra y durante todas las fases de las operaciones militares, asistiendo a un comandante a lograr los principios de sorpresa, seguridad, masa, y la economía de la fuerza, provocando a los adversarios una mala asignación delos recursos en tiempo, lugar, cantidad o eficacia.

El mejor ejemplo que podemos dar sobe el engaño militar es la operación "Fortitude" explicada por Antony, Beevoren su libro el Día D[32]. En esta operación se logro engañar a todo el alto mando Alemán sobre el lugar donde se llevaría a cabo el desembarco de las fuerzas aliadas en Europa, forzando al propio Adolfo Hitler a mantener tropas aferradas en el terreno sobre el paso de Cale al sur de Francia, siendo que el desembarco estaba planificado al norte en las playas de Normandía.

Los planificadores de FORTITUDE partieron del conocimiento y experiencia que tenían sobre las tres principales capacidades de reunión de información con las que contaban los alemanes, para poder detectar, alertar sus defensas y rechazar a la fuerza invasora, estas eran: El espionaje, que se basaba en la amplia red de agentes que los alemanes suponían haber infiltrado en las Islas Británicas; La escucha radial, o sea la

[31]Joint Doctrine for Information Operations – Department of Defense EE.UU – Octubre 1998

[32]Beevor, Antony .El dia D, la batalla de Normandía - E**ditorial Critica**

captación e interpretación del trafico de las comunicaciones radioeléctricas aliadas y finalmente; El reconocimiento fotográfico y la consiguiente interpretación de imágenes de la Luftwaffe

Esta operación duro tres años, donde se utilizaron métodos inimaginables para lograr confundir a los alemanes se crearon ejércitos y flotas fantasmas, se inundaron los medios de comunicación social con información falsa, se comenzó a utilizar el espectro electro magnético para obtener información y enviar información, fueron los albores de la guerra electrónica y la inteligencia humana jugo u rol preponderante donde las redes de espionaje tanto de un bando como el otro marcaron esta actividad hasta nuestros días.

La guerra electrónica: En las operaciones militares, el término Guerra Electrónica (GE), se refiere a cualquier acción militar que involucra el uso de energía electromagnética dirigida para controlar el espectro electromagnético (EM) o para atacar al enemigo. Las operaciones militares en la actualidad se están llevando a cabo en un complejo entorno electromagnético, los dispositivos empleados tanto de uso civil como el militar se utilizan para comunicaciones, navegación, sensores, almacenamiento de información y proceso además de otra gran variedad de usos.

La portabilidad y accesibilidad creciente sumada a las sofisticaciones de los utilizados en el espectro electromagnético garantiza que la operación militar en este ambiente se hará más sofisticado en el futuro.

La necesidad reconocida delas fuerzas militares para tener libre acceso y uso del espectro electromagnético crea vulnerabilidades y oportunidades para la GE en apoyo de las operaciones militares. A la GE se la puede emplear de tres formas "Operaciones de Ataque de GE, Operaciones de defensa de GE y Operaciones de apoyo a la GE"[33], que en su conjunto forman una de las capacidades integradas utilizadas para llevar a cabo operaciones de información (OI) buscando en definitiva negar el uso del espectro electromagnético al enemigo.

En 1944 en la Segunda Guerra Mundial, durante la operación Fortitude antes mencionada, dentro de las operaciones de velo y engaño el ingeniero Austriaco Theodor Suchy, perteneciente a un organismo consagrado al desarrollo de nuevas armas y accesorios, creo una pintura metálica que era buena conductora de electricidad.

Al pintar un globo cautivo con esta pintura, comprobó que producía ecos especiales en los radares, especialmente se probo en los radares con que contaba la

[33] Manual de doctrina conjunta de las Fuerzas Armadas de EE.UU, Publicaciones 3-51, Abril 2000

fuerza Germana donde los ecos recibidos eran idénticos a los reflejados por un crucero pesado o una nave de transporte de unas 10.000 toneladas.

También corroboró que el lanzamiento de pequeñas cintas metálicas lanzadas desde aviones se reflejaban en los radares alemanes, dando la sensación de tratarse de numerosos aviones enemigos.

Concretado el éxito del desarrollo el día 5 de junio de 1944 (día D –1), partieron desde el sur de Inglaterra, rumbo a Francia, una flotilla de lanchas motoras, cada una de las cuales llevaba remolcando consigo dos globos de 9 metros, uno encima y el otro flotando sobre una balsa remolcada. Sobre las embarcaciones volaban bombarderos de la RAF lanzando las tiras de aluminio para engañar al radar.

Al observar las pantallas de los radares, los alemanes quedaron perplejos, una enorme fuerza se cernía sobre ellos. Ante esta situación no solo debieron mantener el orden de batalla en Caláis, sino que, incluso tuvieron que reforzarlo con elementos de la Luftwaffe para oponerse a la supuesta fuerza invasora, induciendo así al alto mando alemán a tomar decisiones erróneas.

3.2Aplicación de la Guerra de la Información.

El manual de doctrina conjunta para la Guerra de la información (Joint Doctrine forInformationOperations) de los Estados Unidos, toma para poder aplicar distintas actividades de la guerra de información, una línea de tiempo dividida en cuatro estadios, paz, crisis, conflicto y paz, dando a cada una de las actividades un nivel normal de esfuerzo, dejando en claro que durante toda la línea de tiempo actúa con C4I (Comando, control, comunicaciones, computación e inteligencia.)

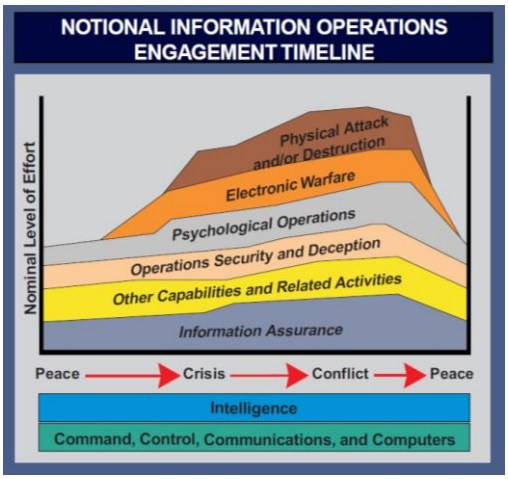

Gráfico N° 2: Operaciones de información sobre una línea de tiempo[34]

[34] Manual de doctrina conjunta de las Fuerzas Armadas de EE.UU, Publicaciones 3-51, Abril 2000.

Como primera medida y durante todo el proceso basa el resto de las operaciones en asegurar la información con que se cuenta, luego continúa con otras capacidades y actividades relacionadas junto con operaciones de velo y engaño, comenzando en el cuarto punto con un incremento de las actividades de acción psicológica

A comienzos de la etapa de crisis el manual marca el inicio de las actividades de guerra electrónica culminando solo en la etapa de crisis y conflicto con ataques y/o destrucción psicológica.

De esta manera vemos como todas las operaciones antes mencionadas utilizadas para llevar a cabo una guerra de la información, son aplicadas por la potencia rectora en este tipo de actividades que apoyados con sus desarrollos tecnológicos han obtenido amplios resultados en esta materia mundialmente conocidos.

Las operaciones han abandonado el ámbito físico o cinético, ahora operan en un ambiente progresivamente, intangible, electrónico. Los ataques pueden ejecutarse a grandes distancias, sin penetrarlos límites de los países, valiéndose a menudo de redes de comunicaciones internacionales. Estas nuevas tecnologías han ocasionado un cambio cualitativo y radical en las formas de agresión.

4.2 Centros de Gravedad (CDG)

Antaño SunTzu hablaba de buscar las debilidades o vulnerabilidades de la defensa del enemigo y que estos debían ser atacados con pequeñas fuerzas altamente movibles. Luego estas teorías fueron tomadas y expuestas por Carl von Clausewitz, años más tarde el coronel JOHN A WARDEN III sugirió que el poder aéreo podría dominar un conflicto, y se impuso la idea de probar que este poder, dirigido contra los "Centros de Gravedad" (CCGG) del enemigo, luego de lograda la superioridad aérea, podría doblegar su voluntad de lucha.

Warden define el CDG como "ese punto donde el enemigo es muy vulnerable y el punto donde un ataque tendrá la mejor oportunidad de ser decisivo."[35]y por misma causa cambiar el curso de la guerra. Al igual que cualquier operación militar, es crucial para la GI antes que se lancen las operaciones definir el centro de gravedad que se desea afectar.

En el nivel estratégico, logramos nuestros objetivos provocando cambios a una o más partes del sistema material del enemigo. Qué parte del sistema adversario

[35]Warden III, Jhon: La campaña Aérea – Escuela Superior de Guerra Aérea – octubre 1991

atacaremos dependerá de cuáles sean nuestros objetivos, cuánto puede el oponente resistir a nuestros esfuerzos o cuán y cuánto poder somos capaces de aplicar material, moral y políticamente.

Su argumento principal es que el poderío aéreo tiene la capacidad singular de atacar en forma simultánea esos CDGs pero la afectación de estos centros de gravedad en la actualidad también se puede llevar a cabo a través de operaciones de ofensivas de la GI con efectos similares, menos destructivos y a un costo militar y político mucho menor.

5.2 Teoría de los Cinco Anillos.

En este punto veremos como el proceso PROMETEO o teoría de los cinco anillos pensado para determinar y afectar centros de gravedad con medios aéreos es aplicable en la guerra de la información.

Este proceso, es un método de acción rápidodecisivo su esencia es simple: pensar estratégicamente, enfocar bien, y moverse rápidamente además permite crear y ejecutar una estrategia única. Le ayuda al Comandante y su Estado Mayor a elegir los objetivos correctos, sus centros de gravedad internos y externos, contra los que pone su energía.

Cada acto y cada cosa ocurre dentro de un sistema y cada cosa que hacemos tiene lugar en el contexto de uno o más sistemas y cada cosa que realizamos afecta a tales sistemas de algún modo. Todos los sistemas poseen centro de gravedad, sin importar cuán simple o complejo sea cada sistema contiene por lo menos un elemento cuya alteración causa un gran impacto sobre el total de estos.

La teoría de los cinco anillos, nos proporciona un buen punto de partida, nos informa cuales son los interrogantes detallados a formular y sugiere una prioridad para las preguntas y las operaciones, desde las más vitales en su centro, hasta las menos esenciales en su exterior.

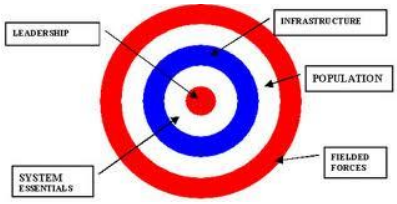

Gráfico N° 3: Cinco anillos de Warden[36]

[36]Smith, Russell J.-Developing an Air Campaign Strategy- *Air & Space Power Journal –noviembre 1999.*

Cada uno de los elementos a los que Warden hace referencia en su pasamiento estratégico, son sensibles de ser afectados por la GI sin la necesidad de utilizar armas para lograr los objetivos planteados.

Su anillo exterior o llamado quinto anillo esta formado por las fuerzas militares, estas pueden ser alcanzadas a través de operaciones de acción psicológica, guerra electrónica, inteligencia y la afectación total de su C2 sin necesidad de emplear armamento. El cuarto anillo es la población la cual es prácticamente imposible atacar directamente, la misma puede absorber un grave sufrimiento antes de que se vuelva contra su propio gobierno ejemplo de esto fueron los ataques sobre Alemania por parte de las fuerzas aliadas.

Nuestros ataques serán entonces sin armas, ya que podremos aunque con un efecto incierto, tratar de llegar a comunicar la información que se considere necesaria para afectar su moral o voluntad de lucha, lográndolo con fuertes operaciones de acción psicológica apoyados por GE que nos permita poder interrumpir en sus dispositivos electrónicos y su vida cotidiana, ejemplo de esto fue que durante la guerra del Golfo en la operación "Libertad Duradera" no solo los soldados, sino los ciudadanos recibían llamados a sus celulares realizados por el fastuoso operativo de propaganda realizado por los EE.UU, solicitándoles que no apoyara a Saddam Hussein[37].

A continuación en el tercer anillo se encuentra la Infraestructura, aquí solo se podrán afectar aquellos centros de gravedad pasibles de ser afectados por la GI o en su defecto se podrán alcanzar a través de ataques indirectos a un subcomponente del CDG.

Con relación al segundo anillo toda la infraestructura critica de una nación (Bancos, Centrales Nucleares, Represas, etc) esta conectada a computadoras muchas veces estos sistemas de transmisión computarizados deben ser tan abiertos y accesibles como sea posible con el fin de utilizar su velocidad y volumen para la eficiencia y eficacia, esta misma apertura es una vulnerabilidad el cual es pasible de un ataque de GI a través de la Ciberguerra.

Durante la guerra de Irak se afectaron las fuentes de generación de electricidad, simultáneamente se invalidaron también la comunicaciones, con esto lograron el efecto

[37] Narváez Rosero, Edison: Guerra Psicológica disponible en: http://www.fuerzasarmadasecuador.org/informacion-variada/guerra-psicologica/ consultada septiembre de 2012.

de anular todo tipo de comunicación, comando y control entre las unidades Iraquíes y logran minimizaron las posibilidad de resistencia de las Fuerzas Iraquíes.

El más crítico es el primer anillo de liderazgo porque se refiere a la estructura de comando enemigo, sea que haya un civil a la cabeza del gobierno o un comandante militar dirigiendo a una flota, sin embargo, se ha hecho muy difícil pero no imposible capturar o matar al elemento de comando, en tal sentido cuando el centro de conducción no puede ser amenazado directamente, la tarea consistirá en aplicar suficiente presión indirecta a los demás anillos que lo rodean por ejemplo las comunicaciones de comando se han hecho más importantes que nunca y por lo tanto son vulnerables al ataque. Cuando estas comunicaciones sufren un daño elevado, como aconteció en Iraq, la conducción tiene grandes dificultades para administrar los esfuerzos de guerra.

Debemos tener en cuenta, que siempre existen un pequeño número de objetivos estratégicos, objetivos estos que tienden a ser pequeños, tienen pocos reemplazos y son complicados de reparar. Si se ataca en paralelo el daño se hace insuperable.

La tecnología ha hecho posible este tipo de ataque casi simultáneo sobre cada nivel de vulnerabilidad estratégico y operacional del enemigo. Asimismo, priva al enemigo de la capacidad para responder con eficacia, y cuanto más grande sea el porcentaje de los objetivos afectados en un solo ataque, menos posible será la respuesta.

Conclusiones

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

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

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

La necesidad por obtener información utilizándola para beneficios propios o en detrimento de un oponente o competidor se ha incrementado en los últimos años, tanto en empresas como en Estados, esto ha llevado a la evolución de nuevos métodos y medios para lograrlo. Esta competencia para obtener información necesaria o vital bloqueando su obtención a la contraparte tanto en el medio civil como militar ha originado una nueva forma de conflicto donde prima la tecnología apoyada con otras tácticas utilizadas antaño.

Esta novedosa forma de guerra ha tirado por tierra antiguos paradigmas de doctrina y empleo basados en antiguos conceptos inaplicables en esta nueva forma de combate. La introducción de las computadoras en todos los órdenes de la vida cotidiana incluyendo los más altos estamentos de un Estado ha generado una vulnerabilidad crítica ya que,sin quererlo, se ha creado un nuevo ambiente donde llevar adelante una contienda:*el ciberespacio*. Esto ha marcado una nueva forma en el desarrollo de las operaciones militares, donde tal vez ya no sean necesarias grandes instalaciones, el empleo de grandes fuerzas o el despliegue de sofisticados medios.

El uso de este ambiente reservado para cierta clase de medios y tecnología disponible solo en grandes potencias durante mucho tiempo, hoy está al alcance de cualquier ciudadano, expresado esto en el exponencial crecimiento durante las últimas décadas del uso de ordenadores e internet.

Este nuevo tipo de conflicto sin armamento,permite al actor más débil poder oponerse al más fuerte con medios adquiribles a un muy bajo costo y con alta

disponibilidad en el mercado civil, donde la afectación de medios tecnológicamente superiores puede ser total, pudiendo anular su ejecución y control.

Si bien existen diversas formas de definir a la Guerra de la Información, todas coinciden en la influencia en que esta nueva forma de combate tiene dentro de un teatro brindando a un Comandante la posibilidad de observar dentro de un Teatro de Operaciones en forma inmediata el terreno, clima, dispositivo de las fuerzas propias (tamaño, ubicación, dirección de empleo, estado operacional, logística) y del dispositivo del enemigo con idéntico detalle.

Es por ello que las operaciones de Guerra de Información sobre el Comando y Control del enemigo tienen un gran valor estratégico ya que tiene como finalidad anular, influenciar, perturbar o retrasar este ciclo de decisión, pudiendo invalidar de esta manera el desarrollo de las operaciones siendo este un punto crucial durante una batalla que, de ser afectado, pondrá en riesgo el desarrollo de cualquier operación militar antes que esta sea lanzada.

Hoy el ciberespacio es el epicentro de las operaciones de GI en tiempo de paz empleando medios emplazados en lugares lejanos, incluyendo redes ubicadas en Estados neutrales que desconocen que han sido infectados por algún virus el cual esta transmitiendo información sensible que afecta los intereses de una nación.

La tendencia de llevar adelante guerras de corta duración, económicas y con un mínimo de bajas humanas, dan un marco ideal para este tipo de conflictos donde operando a través de los ámbitos de Comando y Control, Acción psicológica, Inteligencia, Guerra Electrónica, Ciberguerra y el engaño militar podemos alcanzar objetivos militares sin el despliegue de fuerzas militares o bien, en caso de ser necesario utilizarlas, ello sería en un numero reducido y a un costo mínimo pudiendo afectar los mismos centros de gravedad que una tropa convencional.

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

Mayor Juan RIQUELME

Bibliografía

Manuales.

Information Operations Roadmap Department of Defense US Government 2003

Manual de doctrina conjunta de las Fuerzas Armadas de EE.UU, Publicaciones 3-51, Abril 2000

Joint Doctrine for Information Operations – Department of Defense EE.UU – Octubre 1998

Joint Doctrine for Information Operations – Joint Chiefs of Staff – 1998

Joint Doctrine for Command and Control Warfare (C2W) - Joint Chiefs of Staff – 1996

Manual de doctrina conjunta de las Fuerzas Armadas de EE.UU, Publicaciones 3-51, Abril 2000.

Warden III, Jhon: La campaña Aérea – Escuela Superior de Guerra Aérea – octubre 1991

Libros.

Cyberspace and Information Operations Study Center, Air University, U.S. Air Force 2008.

InformtaionWarfare: Reto E Haeni, profesor de la universidad George Washintong 2006.

James, Adams: La próxima guerra mundial, pp.15-16, Granica, Buenos Aires , 1996

Reto, Haeni. E. Information Warfare: The George Washington University Cyberspace Policy Institute 2033 K Str. Suite 340 N Washington DC 20006

Smith, Russell J. - Developing an Air Campaign Strategy- *Air & Space Power Journal –noviembre 1999*

Keith B, Alexander : «El dominio de los guerreros cibernéticos», *MilitaryInformationTechnology,* volumen 4, número 2, Agence France-Presse, 2011.

Los ámbitos no terrestres en la guerra futura: Espacio - CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL – Monografías del CESDEN – Editado por el Ministerio de Defensa Español – mayo 2012

Piratas Informáticos abren fuego en el ciberespacio, volumen 3, p. 41, Estados Unidos, 2010

James, Adams: La próxima guerra mundial, pp.15-16, editorial Granica, Buenos Aires (Argentina), 1996.

Aldrich, Richard W.: The international legal implications of information warfare, Colorado (EstadosUnidos), Information Warfare Series, USAF Institute for National Security Studies US Air Force Academy, 1966.
Thrasher, Dean Roger: Information warfare Delphi: raw results, p. 4, Monterey, 1996

Documentos electrónicos.

ONU: XII Congreso de Naciones Unidas sobre «Prevención del delito y justicia penal», «La falta de cooperación internacional facilita una vía de escape a los delincuentes cibernéticos.» Salvador (Brasil), 12 a 19 de abril de 2010, Disponible en: http://www.un.org/es/events/crimecongress2010/pdf/factsheet_ebook_es.pdf consultada 20 de junio de 2011
Institute for the Advance study of Information Warfare (IASIW) Disponible en: http://www.psycom.net/iwar.1.htmlconsultada mayo de 2012
Information Warfare, Information Operations and Electronic Attack Capabilities Disponible en: http://www.ausairpower.net/iw.htmlconsultadajunio de 2012
Kuehl, Daniel, T Guerra de Información Estratégica y conciencia amplia de la situación.
Disponible en: http://www.afcea.org.ar/publicaciones/conciencia.htm consultada mayo de 2012
Minoletti Olivares, Jorge Guerra de la Información Disponible en: http://www.afcea.org.ar/publicaciones/infoguerra2.htm consultada mayo de 2012.
Pueyrredon Marcos emprende mundos Disponible en: http://emprende-el-mundo.blogspot.com.ar/2009/06/comercio-electronico-entrevista-con.html consultada septiembre 2012

Narváez Rosero, Edison. Guerra Psicológica Disponible en: http://www.fuerzasarmadasecuador.org/informacion-variada/guerra-psicologica/

Lynn II, William J.: «Defendiendo un nuevo ámbito. La ciberestrategia del Pentágono», Manual de Informaciones, volumen LIII, p. 33, Buenos Aires, junio de 2012, Disponible en: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domainKuehl, Daniel T. Guerra de información estratégica y conciencia amplia de la situación. Disponible en: http://www.afcea.org.ar/publicaciones/conciencia.htm consultada en agosto de 2012

Ley de Defensa Nacional 23.554/88 Disponible en: http://www.mindef.gov.ar/publicaciones/derechos_humanos/Ley-de-Defensa-Nacional.php consultado agosto de 2012.

.