



**“NUEVA ARQUITECTURA  
DE LA  
SEGURIDAD HEMISFERICA”**

- **LA TRANSFORMACION MILITAR DE USA.**
- **LA REVOLUCION DE ASUNTOS MILITARES (RMA).**
- **PRE-EMPTION: NUEVA DOCTRINA ESTRATEGICA.**

**(2° INFORME DE PROGRESO)**

**Septiembre, 2005.**

## **Transformación Militar: Un imperativo ante la amenaza.**

A pesar de que las fuerzas militares de USA tienen ventajas importantes en muchos aspectos ante un conflicto armado existen amenazas que provienen de adversarios que poseen o buscan tener nuevas capacidades o diseñan nuevos conceptos para superar las ventajas de USA. Dentro de un rango de incertidumbre, es posible sin embargo identificar algunas tendencias que podrían permitir que adversarios alcancen capacidades y oportunidades para dañar a los Estados Unidos.

Estas tendencias incluyen lo siguiente en opinión del DoD:

- Disminución de la protección dada por la ubicación y la posición geográfica. Como se ha visto, la posición geográfica de los Estados Unidos no proporciona inmunidad ante un ataque directo a su pueblo, territorio o infraestructura. Los enemigos de USA están buscando nuevos medios para superar las dificultades de las distancias geográficas. Es evidente que hay un número creciente de Estados que poseen o que poseerán misiles cruceros y misiles balísticos de creciente alcance. Mas aún la globalización económica y el incremento de viajes y comercio a través de las fronteras de USA ha creado nuevas vulnerabilidades frente a Estados hostiles o actores que exploten estas oportunidades y pueden perpetrar ataques devastadores al territorio de USA.

- Emergencia de amenazas regionales. Se sabe que existen potencias regionales que están desarrollando capacidades que amenacen la estabilidad en regiones críticas para los intereses de USA. En particular, Asia está gradualmente emergiendo como una región susceptible de competencia militar a gran escala. Así se observa cuando se traza un arco de inestabilidad que va desde el Medio Oriente al Noreste Asiático zona del mundo donde se aprecia una mezcla volátil de potencias regionales en emergencia así como en declinación. Los gobiernos de alguno de estos estados son vulnerables a movimientos y fuerzas políticas internas radicales y, aún, extremistas. Alguno de estos Estados tienen fuertes contingentes militares y pueden poseer, desarrollar y adquirir Armas de Destrucción Masiva (WMD). Por ejemplo Irán y Korea del Norte se están armando con misiles de largo alcance y han adquirido y están buscando adquirir WMD. Estos regímenes continúan apoyando organizaciones terroristas en todo el mundo y mantienen un régimen de terror sobre sus propios pueblos.
  
- Amenazas asimétricas crecientes. En los últimos años adversarios potenciales de USA han intentado balancear la superioridad militar convencional de USA desarrollando capacidades y enfoques asimétricos. Los terroristas han atacado a población no combatiente; otros adversarios han usado armas tales como minas y otras no tan sofisticadas. Como se mencionó, adversarios como Irán y Korea del Norte están invirtiendo en WMD y en un amplio rango de métodos para su uso letal con la esperanza de disuadir o frustrar el despliegue y empleo de las capacidades de combate de USA.

- Amenazas crecientes de Estados débiles o áreas sin gobierno. Distintas áreas de Asia, Africa y aún en el Hemisferio Occidental muestran gobiernos sin capacidad ni responsabilidad que permite a actores o pequeños grupos fuera del Estado (non - state actors) desarrollar actividades terroristas, adquirir armas, traficar drogas y practicar otros ilícitos a través de las fronteras. Este mundo subterráneo dedicado al terrorismo incluye grupos como Al Qaeda, Hamas, Hezbollah, Islamic Jihad, Al Aqsa Martyrs Brigades y Jaish I Mohammed operan en estas áreas. En una era de terrorismo catastrófico los Estados Unidos no pueden ignorar la anarquía que amenaza varias regiones del mundo. En cada caso la incapacidad de algunos Estados para gobernar sus sociedades, salvaguardar su armamento militar e impedir que su territorio se use como santuario para organizaciones terroristas y criminales representa una amenaza a la estabilidad regional y demanda la presencia e influencia de fuerzas de USA]. La reciente historia de Afganistán con el brutal reino de los Talibanes y el desarrollo de bases de entrenamiento y otras facilidades para Al Qaeda es el mejor ejemplo de las implicaciones que tiene para la seguridad de USA la existencia de estas áreas debilitadas o fuera de control de gobierno.

- Difusión de poder militar y capacidades militares de actores o grupos fuera del Estado (non-state actors). Se ha señalado ya que los grupos terroristas o individuos dedicados a estas actividades poseen tanto la motivación como alguna capacidad de realizar ataques devastadores en el territorio de USA o contra sus ciudadanos e infraestructura. En ocasiones estos grupos pueden tener el apoyo de Estados amigos que los protegen y les ofrecen santuario pero algunos tienen los recursos y capacidades para operar sin ningún apoyo del Estado. Al respecto, las redes terroristas y sus grupos de apoyo explotan todas las ventajas de la globalización que ofrece múltiples oportunidades de adquirir o desarrollar diversos tipos de armas.
  
- Creciente diversidad de origen e imprecisión de los sitios de conflicto. Como se aprecia, las tendencias señaladas revelan un panorama geopolítico que es de complejidad creciente e impredecible. A diferencia del pasado, los Estados Unidos no podrá anticipar el desarrollo y ejecución de sus planes militares teniendo un adversario específico y conocido que opera en un área geográfica determinada como fue la URSS. De este modo USA podría enfrentar la necesidad de intervenir en crisis inesperadas contra oponentes dotados de una amplia gama de posibilidades de ataque. En forma adicional estas intervenciones podrían tener lugar en regiones muy distantes y estar sometidas a grandes desafíos operacionales derivados del territorio, el ambiente urbano y aun las condiciones climáticas.

## **La transformación militar como un imperativo de mitigación de riesgos.**

El manejo de riesgos descrito como uno de los siete principios doctrinarios de la estrategia de Defensa es un tema central en la nueva manera de pensar del DoD. Es evidente que en una empresa tan compleja como la del DoD crear un marco de manejo de respuestas a diferentes tipos de riesgos es una tarea esencial. Al respecto, el marco de manejo de riesgos del DoD distingue cuatro tipos de riesgos que afectan la capacidad de Estados Unidos para alcanzar sus objetivos de la política de defensa. Estos son:

- Riesgo del manejo de la fuerza. Este tipo de riesgo proviene de asuntos que afecten la capacidad de reclutar, entrenar, equipar y retener el número adecuado de personal militar de calidad así como sostener el alistamiento de la fuerza para cumplir diversas tareas operacionales.
- Riesgos operacionales. Estos corresponden a los factores que afectan la capacidad de lograr objetivos militares en un conflicto o en otras contingencias.
- Riesgos frente a desafíos futuros. Estos corresponden a asuntos que afecten las decisiones de invertir en nuevas capacidades y desarrollar nuevos conceptos operacionales necesarios para disuadir o derrotar desafíos o riesgos militares de mediano o largo plazo.

- Riesgos institucionales. Son los que derivan de factores que afectan la capacidad de desarrollar prácticas y controles de gestión que permitan usar los recursos del DoD en forma más eficiente permitiendo una más efectiva operación del Departamento.

Cualquier falla de manejo de estas fuentes de riesgo puede poner en peligro las capacidades de USA. En el pasado el Departamento tendió a sobreinvertir en la capacidad de minimizar los riesgos operacionales de la fuerza al entrar en acción mientras se prestó menor atención e inversión a las otras categorías de riesgos, especialmente, en el caso de riesgos emanados de desafíos futuros. El nuevo marco de manejo de riesgos del actual DoD equilibra la atención y proporciona un sistema que asegura una atención balanceada de recursos para mantener una fuerza preparada y lista así como para satisfacer los requerimientos operacionales, las demandas de la transformación de las fuerzas en el futuro y los imperativos de adecuar y modernizar los procesos internos en el DoD.

De este modo la transformación militar de USA es clave para mitigar los desafíos de riesgos emergentes. A la luz de los cambios acelerados ocurridos en el ambiente de seguridad la tarea de manejo de riesgos futuros ha adquirido una alta atención y prioridad. De acuerdo con esto el DoD acepta hoy la necesidad de invertir más en acciones que anticipen o resuelvan desafíos o riesgos futuros. En otras palabras, se ha hecho evidente un desajuste entre el poderío y peso de la fuerza militar de USA y los requerimientos para responder a las capacidades potenciales de futuros

adversarios. El DoD debe ser capaz de decidir inversiones de transformación que estén dirigidas con mayor especificidad hacia riesgos futuros de manera de alcanzar un esfuerzo balanceado en la atención a las otras tres áreas primarias de riesgos. Esto, aunque muchos elementos y componentes de la actual fuerza continuarán siendo una contribución a las capacidades de USA se señala que hay una necesidad creciente de desarrollar nuevas capacidades que den un margen de superioridad. Los sucesos del 9/11 revelaron el peligro de posponer los preparativos para el futuro.

Por último en esta materia se afirma que USA debe prepararse ahora para anticipar sorpresas futuras y poder mitigar sus efectos.

Un breve comentario sobre este capítulo de manejo de riesgos en la transformación militar de USA es la concentración de estos esfuerzos en riesgos de gran escala o alta sofisticación que son el verdadero soporte material de la transformación militar de USA la cual, en el fondo, consiste en afirmar y multiplicar la superioridad militar de USA frente a distintas amenazas. Pero este enfoque de la transformación militar no se aprecia en la práctica concentrando la debida atención de la formidable maquinaria bélica de USA a las tácticas domésticas de grupos terroristas como los de los atentados en Madrid y Londres que no han usado ninguna sofisticación ni armas de destrucción masiva y han provocado conmoción mundial.

## **SEIS OBJETIVOS OPERACIONALES CRITICOS.**

Como se ha señalado en esta revisión el propósito de la transformación militar de USA es mantener o mejorar la superioridad militar del país frente a un ambiente de seguridad impredecible y potencialmente sujeto a grandes cambios. Así concebida la transformación militar debe concentrarse en los desafíos emergentes de tipo estratégico y operacional así como en las oportunidades creadas por estos desafíos. Frente a esta tarea el Secretario de Defensa ha identificado seis objetivos operacionales críticos en los que se focalizan los esfuerzos de transformación del DoD. Se trata entonces de esfuerzos que desarrollen las capacidades necesarias para alcanzar estos objetivos operacionales permitiendo ampliar las capacidades de las fuerzas de USA.

Los seis objetivos críticos del DoD son :

- Proteger bases criticas y derrotar las Armas de Destrucción Masiva (WMD)
- Proyectar y sostener fuerzas
- Negar santuario al enemigo
- Incrementar la tecnología de información
- Asegurar los sistemas de información
- Reforzar la capacidad espacial

## **Proteger bases críticas y derrotar armas de destrucción masiva (WMD).**

En primer lugar, las fuerzas militares de USA deben proteger las bases de operaciones críticas y derrotar el uso de armas de destrucción masiva. El territorio doméstico de USA es la base más importante a proteger y defenderlo de ataques exteriores es la mayor responsabilidad de las fuerzas armadas de USA. Ni los vastos océanos ni los buenos vecinos aíslan a Estados Unidos de ataques que emanen del exterior. Los ataques del 11 de Septiembre revelaron la vulnerabilidad frente a ataques terroristas de la sociedad abierta que caracteriza a la Nación. Las letales cartas con antrax enviadas el otoño del 2001 demostraron, a su vez, el grave peligro potencial de terroristas poseedores de armas de destrucción masiva (WMD).

De este modo los adversarios futuros disponen de una variedad de nuevos medios y formas con los que pueden amenazar a Estados Unidos tanto en su territorio como en el exterior. Como se ha dicho, estos medios incluyen nuevas formas de terrorismo, armas de destrucción masiva más avanzadas, misiles cruceros y balísticos y armas de efectos masivos como los de ataque a la infraestructura de información. El DoD está trabajando en estos desafíos operacionales emergentes. Por ejemplo, ha reorientado su programa de misiles defensivos para proteger mejor el territorio de USA y ha desplegado fuerzas, aliados y amigos para protegerlos de misiles balísticos de cualquier alcance. En otra área se están apoyando programas de ciencia y tecnología destinados a defenderse contra amenazas biológicas.

## **Proyectar y sostener fuerzas.**

Se ha dicho que los adversarios potenciales buscan alcanzar capacidades que puedan anular parte de la actual capacidad militar de USA para proyectar poder militar a distancia. En la actualidad la proyección de fuerza de USA depende en gran medida en tener acceso a grandes bases, aeropuertos y puertos ubicados en diversas partes del mundo. Un ataque con misiles balísticos o crucero armado con cabezales conteniendo WMD podría alterar gravemente o impedir la entrada de fuerzas de USA en un teatro de operaciones. A su vez un sistema de defensa anti-aérea avanzado podría negar el acceso a un ataque aéreo hostil e impedir las operaciones de guerra aérea. A su vez a través de radares y otras capacidades espaciales así como vehículos aéreos no piloteados (UAV) podrían permitir a adversarios potenciales tener grandes áreas bajo vigilancia y detectar y atacar fuerzas de USA. Además, teniendo submarinos convencionales, misiles de superficie y minas marinas podrían alcanzar capacidades y usos que amenacen la capacidad de las fuerzas navales y anfibias de USA para operar en aguas del litoral.

Frente a todas estas amenazas se necesitan nuevos enfoques para mantener la capacidad de proyectar fuerzas de USA. Estos enfoques deberán concentrarse en reforzar las defensas activas y pasivas de USA contra ataques de misiles y WMD; en distribuir fuerzas a través de un teatro de operaciones y desarrollar nuevos conceptos de combate; en reducir la dependencia de uso de puertos y bases y en aumentar la “invisibles” en el uso de vehículos aéreos hipersónicos, no manejados por pilotos, y de largo

alcance que permiten proyectar poder. A la vez, se debe reforzar la capacidad de proyectar y mantener fuerzas directamente desde una plataforma marítima integrada. Además, se debe desarrollar fuerzas terrestres que sean más livianas, más letales, más versátiles, más sostenibles y de despliegue rápido.

Como se aprecia de la reciente descripción se trata de un formidable esfuerzo de cambio y de logística cuyo solo enunciado tiene requerimientos de largo alcance y complejidad

### **Negar santuario al enemigo.**

En otro ámbito de acción el adversario puede buscar operar en vastos territorios usando sistemas móviles y escondites a su elección. Se sabe que los sistemas de misiles balísticos móviles pueden desplazarse y ser disparados desde grandes distancias negando el acceso a áreas de conflicto. Hay otros sistemas como los rayos láser empleados desde tierra que pueden ubicarse en lugares remotos pero tener capacidades de daño espacial. Ante este cuadro la transformación tiene un objetivo clave cual es desarrollar medios para impedir el uso de territorios o santuarios por parte de adversarios potenciales en cualquier parte del mundo. Esto requiere el desarrollo y adquisición de grandes capacidades para una vigilancia continua de vastas áreas geográficas así como una capacidad de ataques de precisión de largo alcance que sean capaces de controlar y rechazar los esfuerzos del adversario.

Además de lo señalado anteriormente la tarea de impedir el uso de territorio o santuarios por el enemigo requerirá también la capacidad de emplear operaciones especiales y otras fuerzas de maniobra en estas áreas y conectarlas con una campaña de ataque de precisión de largo alcance. Al respecto se señala el ejemplo de Afganistán e Irak donde la combinación de fuerzas terrestres con ataques de precisión de largo alcance se demostró como exitosa. Estos casos son una visión del potencial que tienen las operaciones integradas si son bien explotadas por los esfuerzos de transformación y experimentación de USA.

### **Incrementar las Tecnologías de Información (IT).**

Las fuerzas de USA deben incrementar las tecnologías de información (IT) así como desarrollar conceptos innovativos de “network – centric operations” ya analizados en este trabajo para tener fuerzas conjuntas más capaces y efectivas. Las nuevas tecnologías de información y comunicaciones permiten conectar en red fuerzas conjuntas y multinacionales desplegadas en distintos puntos en un teatro de operaciones que permitan a estas fuerzas tener una mejor información de la situación tanto de fuerzas amigas como adversarias. Los sistemas de comando, control, comunicaciones, computadores, inteligencia, vigilancia y reconocimiento potencian el poder combatiente a través de la conexión en red dada por plataformas, armas, sensores y controles que actúan coordinadamente teniendo una visión común del campo de batalla.

En la guerra de Afganistán, Estados Unidos demostró la capacidad de atacar desde larga distancia a través de una variedad de elementos de combate conectados con los Servicios. Esto incluyó a Fuerzas Especiales de todos los Servicios, a los bombarderos intercontinentales de la Fuerza Aérea, a elementos de dos divisiones del Ejército, varios grupos de combate de portaviones y unidades expedicionarias de Infantes de Marina. Sin embargo este ejemplo de acción conjunta solo vislumbra el potencial de oportunidades que puede representar la conexión de fuerzas de aire, mar y tierra actuando conjuntamente de una manera nueva e innovativa..

Las tecnologías de información (IT) tienen un vasto potencial para maximizar la efectividad de las fuerzas de USA. Se reitera la necesidad de moverse hacia el llamado “network – centric warfare”, incrementar la importancia de la conectividad y de la interoperabilidad como factores críticos cuando se diseñan o adquieren los equipos de comando, control, comunicaciones y computadores y sistemas de armas. Se señala asimismo que el DoD debe mejorar su procedimiento de supervisión de sus procesos de requerimientos, programación y adquisiciones de manera que se amplie el rango de capacidades de todo el material que adquiere. Se recalca que el objetivo es permitir que las fuerzas de USA estén mejor comunicadas entre sí, mantengan una continúa información de las posiciones de fuerzas amigas neutrales o enemigas y compartan el mismo cuadro preciso en tiempo real de lo que ocurre en el campo de batalla.

### **Asegurar los sistemas de información.**

Los sistemas de información deben estar protegidos de ataques de adversarios y se debe desarrollar nuevas capacidades de operaciones de información más efectivos. La emergencia de redes avanzadas de información abre un promisorio campo de mejoras en las capacidades conjuntas de USA a la vez que proporciona herramientas para ataques de USA desde posiciones fijas del tipo guerra electrónica o psicológica.

Sin embargo la creciente dependencia de las sociedades y de las fuerzas militares en las redes de información crea nuevas vulnerabilidades. Esto puede ser aprovechado por adversarios potenciales para preparar sus propios ataques a través de redes de computación. Estos ataques a las redes de información se ven facilitados por la amplia penetración mundial alcanzada por el mundo cibernético como asimismo por el descenso de los costos y la difusión de estas tecnologías. De allí que para proteger la actual ventaja en sistemas de información de USA se requiere una mayor coordinación de las capacidades ofensivas y defensivas así como una integración más efectiva de estas capacidades con las actividades de inteligencia.

### **Reforzar la capacidad espacial.**

El Departamento de Defensa debe potenciar la capacidad y sobrevida de sus sistemas espaciales. Las actividades conducidas en el espacio son criticas para la seguridad nacional y el bienestar económico de la Nación. Tanto los amigos como los adversarios potenciales serán cada día más dependientes de sistemas espaciales que permiten las comunicaciones, detectar posiciones, navegación y otros datos. Además de explotar el espacio para su propio uso los potenciales adversarios podrán intentar impedir a las fuerzas de USA el acceso y uso para operar a través o desde el espacio. En el futuro se prevé que la vigilancia espacial, las bases del láser terrestre, la capacidad de alterar la comunicación en el espacio y el acceso a micro-satélites será posible alcanzarlo por muchos actores. De allí que el objetivo clave de la transformación sea mantener las variadas ventajas que tiene USA en materia espacial pero también cerrar las vulnerabilidades espaciales que puedan dar margen a nuevas formas de competencia en el espacio. Las fuerzas de USA deben asegurar el control del espacio y deben garantizar la libertad del país para actuar en el espacio en tiempo de conflicto.

## **LOS CUATRO PILARES DE LA TRANSFORMACION MILITAR.**

Como se ha repetido, el propósito central de la transformación estratégica de USA es permitir al DoD manejar mejor dos grandes desafíos de transformación que en ambos casos requieren invertir en estas tareas. El primer desafío de transformación es la necesidad de invertir ahora en tecnologías específicas y conceptos que faciliten la transformación. Para transformar la fuerza se debe comprometer recursos permitiendo continuar un proceso iterativo de innovación y experimentación que estimule nuevas visiones que guíen otras decisiones de inversión futura.

El segundo desafío de transformación es la necesidad de balancear las necesidades operacionales más inmediatas con las decisiones de inversión en riesgos futuros o emergentes. Posponer grandes inversiones en transformar capacidades militares dedicando la mayor parte del gasto para atender las necesidades operacionales más inmediatas hace correr el riesgo de ser sorprendido por adversarios más creativos y dedicados. Por lo tanto para progresar en la transformación militar se requiere importantes inversiones en aquellos aspectos de transformación que se crea más seguros de reportar beneficios más duraderos. Aún en un ambiente de presupuestos de Defensa en crecimiento los dólares son limitados. De acuerdo con esto puede resultar un efecto de cancelación o de reducción importante de gastos en ciertos sistemas para aumentar la inversión en capacidades que se crea podrán reducir riesgos futuros.

## **COMPONENTES ESENCIALES DE LA ESTRATEGIA DE LA TRANSFORMACIÓN MILITAR.**

La estrategia general de transformación militar del Departamento de Defensa consiste en tres partes:

- Transformar la cultura del DoD
- Transformar los procesos del Departamento
- Transformar las capacidades de la fuerza

Al comienzo del proceso transformador el Departamento de Defensa focalizó estas cuestiones en lo que denominó los Cuatro Pilares de la Transformación Militar. Estos cuatro pilares constituyen elementos esenciales de la estrategia de transformación de la fuerza militar en el DoD. Estos son:

- Reforzar operaciones conjuntas;
- Explotar la superioridad de inteligencia de USA;
- Desarrollar y experimentar nuevos conceptos;
- Desarrollar nuevas capacidades de transformación

El significado de una implementación exitosa de la estrategia de la transformación militar equivaldrá a un giro desde la era industrial a una era de información a nivel militar de modo que las futuras operaciones militares serán conducidas con fuerzas basadas en enfoques tipo “network – centric warfare”. Asimismo las operaciones deberán distribuir fuerzas con mayor alcance y amplitud utilizando una información común a través de una red de seguridad que entregará información de las acciones a todos los niveles de comando. A su vez, esta información compartida creará condiciones para aumentar la velocidad de decisiones de comando y de las oportunidades de acción sincronizada en el campo de batalla. El primer paso hacia el desarrollo de una fuerza conjunta trabajando bajo el concepto de “network – centric warfare” es aumentar ahora la inversión en los cuatro pilares reseñados de la transformación militar. El objetivo de todos estos esfuerzos es producir fuerzas militares que tengan las siguientes capacidades al final de esta década:

- Efectos confirmables y planificación adaptada. Los cuarteles generales de fuerzas conjuntas prontas a la acción conducirán acciones medidas por sus efectos a través de un planeamiento adaptado a los objetivos así como para responder a contingencias con el objetivo de derrotar las amenazas enemigas usando fuerzas interconectadas a través de diferentes módulos y capaces de desarrollar operaciones conjuntas y combinadas.

- Proyección de poder en ambientes hostiles. Las fuerzas de USA deben ser capaces de derrotar cualquier capacidad del enemigo para negarle acceso o rechazar la presencia de USA a través de una combinación de medidas de prevención en ambientes contaminados, usos de bases móviles y prioridad de uso rápido en contrataques.
  
- Incrementar ventajas asimétricas. Las fuerzas de USA deberán incrementar las ventajas asimétricas de la Nación hasta el máximo posible a través de un empleo a fondo de sus capacidades de comando, control, comunicaciones, computadores, inteligencia, vigilancia y reconocimiento (todos estos elementos se designan en inglés como C4ISR de manera de tener alcance global, conocimiento común de la situación operacional en el campo de batalla, un rápido y robusto sistema de ajuste de blancos y los indispensables requisitos para conducir operaciones bajo el enfoque del “network – centric warfare”. Este nuevo concepto está explicado al comienzo de este informe (página 27).
  
- Maniobras conjuntas y combinadas. Con todo lo señalado la fuerza militar podrá desarrollar operaciones conjuntas y combinadas contando con una mejor visión de la situación que les permitirá maniobrar más fácilmente frente a los obstáculos del campo de batalla y forzar al enemigo a una respuesta masiva que permita el máximo uso de la capacidad de ataques de precisión.

Con estas capacidades las fuerzas militares de USA estarán en mejores condiciones de acometer y lograr los seis objetivos operacionales debatidos en capítulos anteriores de este estudio. De este modo comprometer una variedad de inversiones prioritarias destinadas a cumplir estos objetivos permitirá ejecutar la nueva estrategia de defensa y establecer una sólida base para nuevas transformaciones.

Sin embargo, se advierte que el proceso de transformación debiendo ser integral y alcanzando desde el área de la ciencia y la tecnología hasta las capacidades en terreno no requiere ser implementado a través de todas las fuerzas militares simultáneamente. Algunos aspectos de la transformación debieran ser de amplia aplicación tales como la mayor conectividad en redes. A su vez la tensión entre la flexibilidad en la transformación y la necesidad de invertir ahora en nuevas capacidades se debe reducir fijando metas. Por ejemplo tenemos la meta de interconectar por redes toda la fuerza pero añadimos una carga a esta red a través del uso de nuevas plataformas en forma deliberada. Así las fuerzas llamadas “vanguardia” que están equipadas con nuevas plataformas serán capaces de explotar estos nuevos conceptos y capacidades en distintos ambientes operacionales e influenciar el desarrollo del resto de la fuerza. De este modo a partir de una inversión en una parte pequeña de la fuerza demostrará que en operaciones reales y ensayos de campo una masa crítica no muy grande de transformación de capacidades militares puede producir y multiplicar efectos favorables que debieran convencer la decisión de aumentar las inversiones a un tamaño mayor de fuerzas.

## **PRIMER PILAR: Reforzar las operaciones conjuntas**

El primer pilar de la transformación militar consiste en reforzar las operaciones conjuntas a través del desarrollo de nuevos conceptos y arquitectura y de intentar otras importantes iniciativas conjuntas y objetivos de interoperabilidad de la fuerza.

Se señala que el desarrollo de conceptos operativos conjuntos en el futuro será clave en la estrategia de la transformación del DoD. Estos nuevos conceptos deberán ser lo suficientemente específicos para permitir la identificación y la priorización de los requerimientos de transformación dentro del programa de Defensa, sin perder la flexibilidad necesaria para absorber nuevas ideas valiosas que emerjan en el camino. Se recalca que en ningún momento una determinada operación conjunta pueda abortar la discusión y la investigación de conceptos alternativos. Al respecto se recuerda que la historia militar ha probado que cuando un concepto operacional alcanza el nivel de “solución única” esto interrumpe el trabajo intelectual en nuevos desarrollos y expone a la fuerza a ser superada por sus competidores.

En relación a los conceptos conjuntos se distinguen tres etapas en el tiempo:

- Operaciones conjuntas de corto plazo (2-3 años). En este caso los Comandantes del teatro de operaciones hacen sus planes con la debida cuenta de las lecciones aprendidas en otras acciones y en el tipo de entrenamiento necesario en un marco de doctrina conjunta, todo esto

diseñado para alcanzar los objetivos estratégicos de manera que el esfuerzo conjunto y las modificaciones en los planes operativos provoquen procesos de transformación militar. En este mismo caso los Comandantes combatientes desarrollan planes de guerra que tienen en cuenta un concepto de operación conjunta de mediano plazo, incorporan las lecciones aprendidas en sus propias operaciones, realizan entrenamiento y ejercicios conjuntos y emplean las mejores tecnologías de uso militar conocida o experimentada.

Sin embargo los planes de guerra y la doctrina conjunta hechos bajo este marco son un punto inicial pero no un estándar común que no invalida como se ha dicho, la experimentación continua ni el desarrollo de nuevos conceptos a futuro.

- Conceptos conjuntos de mediano plazo. En este caso se trata de diseñar conceptos conjuntos que visualicen como se preparará para combates futuros la acción conjunta de la fuerza. En suma, se tratará de identificar tipos específicos de operaciones militares seleccionadas a través del amplio rango de acciones de este tipo. En todo caso esta acción de mediano plazo deberá ser diseñada de acuerdo con los seis objetivos operacionales críticos del DoD (ya reseñados). Entre estas acciones se distingue:

- Concepto de operación conjunta. En este punto se indica que la transformación militar se logra ligando la construcción estratégica con una aplicación integral de las capacidades de una fuerza conjunta. El detalle de estos conceptos de operación conjunta se encuentra en otros documentos del DoD. Sin embargo se señala que este enfoque conceptual conjunto será el marco futuro que guiará las operaciones conjuntas y todo el desarrollo y experimentación del apoyo a la actuación conjunta de los Servicios. A la vez este marco orientará el desarrollo y adquisición de nuevas capacidades militares a través de cambios en la doctrina, organización, entrenamiento, equipamiento, liderazgo y educación, personal y otras facilidades.
  
- Conceptos de acciones operativas conjuntas. En el caso recién descrito los conceptos de operación conjunta tienen un contenido doctrinario y de organización mientras que en el caso de conceptos para acciones operativas conjuntas el foco se concentra en el nivel operativo mismo en terreno. Así en esta área se describe como un Comandante de una fuerza conjunta planeará, preparará, desplegará, empleará y sostendrá una determinada fuerza conjunta para actuar en una operación específica o en una combinación de operaciones. Para una mejor visualización de estos conceptos aplicados a la acción se señala que este tipo de operaciones conjuntas se están desarrollando en cuatro campos de acción que son la seguridad interior, la operación en grandes conflictos bélicos, las operaciones llamadas de estabilización

y, por último, las operaciones destinadas a la situación del llamado “deterrence estratégico”. Como se aprecia de este listado estos cuatro campos de acción son los escenarios de mayor prioridad e importancia para USA y es útil tomar nota que en estas áreas tan sensibles el enfoque futuro es a través de dos conceptos fundamentales como es la acción conjunta y la interoperabilidad de las fuerzas. Estas tendencias recientes y en plena evolución deben ser cuidadosamente consideradas a nivel interno de Chile

Asimismo se señala que todos estos conceptos conjuntos deben evolucionar en el tiempo para incorporar nuevas visiones obtenidas a través de la experimentación continua. La hoja de ruta de la transformación de los Servicios deberá identificar las capacidades operacionales necesarias para implementar estos conceptos y operaciones conjuntas así como los mejores medios y procedimientos para obtener estas capacidades.

- Arquitectura y capacidades integradas. El concepto de arquitectura describe hasta el detalle la relación existente entre las tareas y las actividades que generan efectos en las fuerzas enemigas y en las operaciones de apoyo. De esta manera el concepto de arquitectura identifica las necesidades materiales de desarrollo de operaciones, los puntos donde las operaciones se pueden entrecruzar o sobreponer y entrega detalles de los requerimientos de los elementos para la interoperabilidad de las fuerzas. Pero el contenido de la denominada “arquitectura en el área militar” no incluye solo soluciones materiales

sino también doctrina, organización y requerimiento de entrenamiento. En base a todos estos componentes integrados en un diseño de arquitectura militar se puede discernir que capacidades son prioritarias para la mejor contribución y realización de las Operaciones Conjuntas.

- Visión conjunta de largo plazo (15-20 años). El DoD ha formulado un documento llamado “Visión Conjunta” que es un documento sobre la articulación a largo plazo de Operaciones Conjuntas. Esta guía hace un amplio desarrollo de los conceptos conjuntos en su evolución futura así como de las capacidades requeridas en las operaciones del futuro. Al mismo tiempo este documento “Visión Conjunta” dedica atención a desarrollar y experimentar en el futuro nuevos conceptos de acción conjunta de los Servicios.
  
- Otras iniciativas conjuntas y objetivos de interoperabilidad. En este punto se señala que una mayor interoperabilidad es un pre-requisito clave para reforzar la acción conjunta y un imperativo para la transformación de la fuerza. Hoy el Departamento de Defensa está ejecutando un proceso de fortalecimiento de operaciones conjuntas a través de una mejor acción de comando y control conjunto, y entrenamiento conjunto a la vez que expandiendo la presencia de fuerzas conjuntas en el mundo. Al mismo tiempo se está usando los resultados de diversos estudios de la interoperabilidad de la fuerza que permita alcanzar las siguiente prioridades interoperativas:

- Procedimientos operativos estándar y proceso de despliegue conjunto, organización y uso de sistemas.
- Visión operacional común y relevante a disposición de las fuerzas conjuntas.
- Refuerzo de las capacidades de inteligencia, vigilancia y reconocimiento.
- Selección de conexiones de “sensor- a -disparador” (sensor-to-shooter) priorizados como una contribución a la acción de campo de las fuerzas conjuntas. (La ligazón de “sensor-to-shooter” se refiere a la capacidad de monitorear y emplear la información de sensores con una respuesta de ataque o contra ataque de sistemas de armas amigos).
- Capacidades que permiten el acceso a sistemas de información global (satélites).
- Planificación “adaptada a la misión”, ensayo y entrenamiento conjunto.

## **SEGUNDO PILAR: Explotando las ventajas de Inteligencia de USA.**

La nueva estrategia de defensa descansa sobre la base y necesidad de transformar las capacidades de inteligencia. La capacidad de defender USA en el nuevo ambiente de seguridad requiere nuevas capacidades de inteligencia de un nivel sin precedentes para anticipar donde, cuando y cómo los adversarios intentarán sus ataques. La visión futura de una fuerza conjunta más pequeña, más letal y más rápida capaz de derrotar a un adversario en cualquier campo de batalla descansa en este tipo de capacidades.

A pesar que hoy en día USA posee mejores sistemas de inteligencia que cualquier adversario potencial se está llevando a efecto numerosos esfuerzos para mejorar y expandir las actuales capacidades de inteligencia. Al mismo tiempo está creciendo la dependencia de las fuerzas militares de USA en sus capacidades de inteligencia. Esto comprende la explotación de las ventajas de USA en esta materia a través de múltiples maneras de recolectar información, observación, vigilancia y reconocimiento global y refuerzo de la explotación y diseminación de estos datos.

- Creciente demanda de capacidad de Inteligencia. Es publico y notorio la critica asociada a la mayor demanda de las capacidades de inteligencia. Del mismo modo, los adversarios potenciales sufren la misma demanda de mayor y mejor información por lo que buscan adquirir capacidades o ventajas similares. En este esfuerzo del adversario ellos persiguen a la

vez estrategias asimétricas incluyendo información operativa de guerra espacial y de uso de armas de destrucción masiva (WMD). Estas amenazas asimétricas son altamente peligrosas y representan desafíos de inteligencia muy amenazadores. Como respuesta, el DoD trabaja arduamente en nuevos procesos y procedimientos que mejoren la eficacia de los sistemas existentes de coleccionar información e intenta desarrollar nuevas tecnologías en este campo. Así, hoy día el DoD considera a las operaciones de inteligencia, información y capacidades espaciales como un núcleo duro que asegure mejores capacidades en operaciones futuras.

- Requerimientos para transformar las capacidades de inteligencia. La inteligencia y su uso oportuno es la primera línea de defensa contra los terroristas y contra las amenazas proveniente de Estados hostiles. En los años de la Guerra Fría la inteligencia estaba focalizada en la prioridad de coleccionar enormes cantidades de información sobre un inmenso territorio pero inmóvil como era el bloque soviético. Esto ha cambiado hacia un panorama donde la comunidad de inteligencia enfrenta el desafío de un mayor número y complejidad de objetivos en el mundo. De aquí emana la necesidad de transformar las capacidades de inteligencia del DoD para mejorar o rediseñar los sistemas de inteligencia de modo que alcancen el punto de alerta mas temprano posible. Al respecto se insiste que en un mundo plagado de amenazas terroristas con acceso a WMD ni USA ni sus aliados pueden permitir que el enemigo golpee primero.

Con estos desafíos de gran envergadura se señala que las capacidades de inteligencia del DoD a lo largo de la próxima década deben ser más proactivas, intrusivas, interconectadas, integradas y rápidas. El DoD está realizando un gran gasto de inversión en este campo especialmente en aquellas acciones que preparan la inteligencia y las operaciones de las fuerzas. Se considera que estas inversiones son críticas como requisitos para alcanzar la inter operabilidad de fuerzas conjuntas para alcanzar sus objetivos. A la vez estas nuevas inversiones en inteligencia son necesarias para mejorar los sistemas de alarma ante crisis emergentes, para identificar blancos críticos en un conflicto, para medir y monitorear el progreso de una campaña y para el proveer indicadores de éxito.

- Inteligencia global. Como se ha dicho los requerimientos de inteligencia actuales son proporcionar a los líderes políticos y militares una información estratégica y operacional dentro de un rango de acción global que comprende entre otros elementos:
  - Inteligencia humana (Humint). Las experiencias ganadas durante los últimos conflictos de Guerra del Golfo, Afganistán e Irak y en la guerra contra el terrorismo han reforzado el valor y la necesidad de mejorar la inteligencia humana. Así la recolección, análisis e informes recogidos por la Humint debe optimizarse para tener acceso y visión “desde dentro” en alguno de los más difíciles y peligrosos blancos como ser células terroristas, blancos subterráneos profundos o planes

de despliegue o uso de WMD. USA necesita reforzar sus capacidades de inteligencia humana (“Humint”) y su instrumental para no sólo anticipar la acción adversaria sino también para mejorar la sinergia de los sistemas de colección de datos con un mejor posicionamiento de fuerzas. Esto significa que los informes provenientes de la “Humint” deben estar más integrados para reforzar la apreciación de la situación y la visión del teatro de operaciones de las fuerzas conjuntas.

- Tecnologías emergentes. El DoD trabajará vigorosamente en el desarrollo y explotación de tecnologías que puedan mejorar la ventaja de USA en la recolección, análisis y seguridad de los sistemas de inteligencia. Algunas de estas nuevas tecnologías son:
  - Tecnologías de observación a baja distancia que pueden emplearse en plataformas para uso de inteligencia.
  - Nanotecnología que pueden producir sensores autónomos de tamaño miniatura, móviles y capaces de penetrar instalaciones remotas y de seguridad de un adversario
  - Sensores interconectados pero difíciles de ubicar que pueden proporcionar las fuerzas amigas información continua altamente precisa y con entrega en tiempo real de las fuerzas enemigas en el campo de batalla.

- Avances en un procesamiento simultáneo computarizado que descifre, traduzca y transcriba las comunicaciones en un proceso en tiempo real.
- Uso de procedimientos biométricos para detectar adversarios así como para identificar personas en instalaciones de seguridad.
- Recolección de imágenes de los sistemas comerciales de sensores remotos del planeta (satélites).

## **Inteligencia, Vigilancia y Reconocimiento.**

El DoD está llevando a cabo una estrategia de inversión en planes que permitan contar con una mezcla integrada y eficiente de aeronaves no pilotadas (unmanned); plataformas pilotadas y sistemas espaciales, marítimos y terrestres capaces de recolectar información de acuerdo a las necesidades futuras. A medida que estas estrategias y planes se desarrollan se necesita una integración horizontal de los contenidos y procesos de inteligencia y vigilancia junto con cambios organizacionales. Actualmente se están desarrollando esfuerzos para adquirir plataformas y sensores para montarlos en vehículos aéreos no pilotados (UAV). Se está requiriendo asimismo sistemas más avanzados de sistemas de radares espaciales que entreguen información de áreas y blancos fijos o móviles usando la capacidad de vigilancia global y de largo alcance de estos sistemas basados en el espacio que tienen mejor capacidad que los sistemas de radares aéreos existentes. A su vez, se está integrando al sistema de información, vigilancia y reconocimiento de USA a los sistemas comerciales de satélites orbitales en uso en la actualidad.

- Sensores. Respecto de estos elementos se destaca la necesidad de contar con un amplio rango de inteligencia de imágenes (IMINT), inteligencia de señales (SIGINT) y de sensores denominados de inteligencia de medida e identificación (MASINT). Los sensores de imágenes satelitales (IMINT) sirven para entregar capacidades de observación muy precisas durante un tiempo. Mientras los sensores de señales (SIGINT) se

necesitan para montarlos en vehículos no piloteados de reconocimiento y en buques cuyos sensores puedan captar señales de radio provenientes de diferentes tipos de amenazas. Se recalca que se necesita una modernización de los sensores de señales (SIGINT) para entregar capacidades de recolectar información de señales de alta y baja frecuencia eludiendo los sistemas de detección. Por su parte, los sensores de medida e identificación ofrecen un amplio rango de aplicaciones potenciales en particular en su capacidad de seleccionar y detectar información sobre instalaciones o blancos subterráneos o muy protegidos todo lo que convierte a esta información en datos críticos para mantener la superioridad militar de USA.

- Operaciones de inteligencia, vigilancia y reconocimiento. Se destaca que estas operaciones conocidas por sus siglas ISR (intelligence surveillance and reconnaissance) deben interactuar con un sentido de empresa de colaboración para lograr responder a las necesidades y al apoyo de las autoridades civiles y Comandantes involucrados en el planeamiento y ejecución de las operaciones. Esta necesidad de cooperación de estas capacidades ISR permiten estrategias, planes y operaciones ágiles y adaptadas al objetivo así como una rápida entrega de análisis y de información crítica en el tiempo entre quienes deben compartir estos datos. Con un cuadro de información de estos sistemas y sensores los líderes y comandantes deben tener una información confiable cercana a un tiempo real que resultará vital para apoyar operaciones y tener una visión completa del espacio operacional. De este

modo todas estas ayuda de sensores y otras herramientas de inteligencia se necesitan para permitir el desarrollo de una estrategia y planes coherentes y una capacidad de introducir ajustes en breve tiempo ante situaciones emergentes. De allí que estos sistemas ISR son esenciales para establecer un sistema de recolección de datos efectivo, eficiente y que responda a estas necesidades de información en operaciones conjuntas y combinadas.

- Tarea, colección, análisis y uso. Las operaciones militares futuras deberán ser de más agilidad y rapidez en el tiempo y, por lo tanto, requerirán innovar los enfoques de uso de la información. Esto significa que se deberá integrar con más efectividad todos los tipos de inteligencia, (IMINT, SIGINT, MASINT y HUMINT) de manera que se pueda tener acceso en breve tiempo y se comparta la información ya analizada entre todos los que deben tener acceso a ella. En la práctica esto significará modificar el modelo secuencial de trabajo de inteligencia, de tarea, recolección, procesamiento, análisis y diseminación con un circuito dado por las funciones, tarea, puesto, procesamiento y uso.

### **Tercer Pilar. Experimentación y Desarrollo de Nuevos Conceptos.**

El Tercer Pilar comprende la experimentación con nuevos enfoques al modo de combatir, a nuevos conceptos operacionales y relativos a las capacidades y diseños organizacionales. Esta experimentación se desarrollará a través de juegos de guerra, simulaciones y ejercicios de terreno focalizados hacia desafíos y oportunidades emergentes. Se da como ejemplo de esta experimentación la unidad constituida por el Ejército de USA llamada Brigada Interina de Equipos de Combate.

El desarrollo de nuevos conceptos y la experimentación son conceptos interconectados. A la aparición de un nuevo concepto debe seguir una experimentación que permita evaluar sus resultados y ayude a refinar o ajustar esos conceptos de una manera continua o iterativa. De este modo el proceso de experimentación consiste en el uso de experimentos con objetivos conjuntos limitados pero interconectados en red con todos los comandantes combatientes. El DoD ha puesto en marcha el desarrollo de múltiples conceptos conjuntos y de acción de los servicios pero conducidos por los comandantes combatientes y los Servicios de manera que exista una competencia de ideas. Esto se ha recogido en un documento llamado “Guía de Planeamiento de la Transformación” que contiene una detallada descripción del desarrollo de nuevos conceptos conjuntos y de la necesaria experimentación.

- Para aclarar mas este desarrollo de nuevos conceptos conjuntos y de la necesaria experimentación en el DoD, su Oficina de Transformación de la Fuerza hizo publico algunos criterios para contar con programas de experimentación exitosos. Estos criterios comprenden las siguientes áreas:
  - El rol del método científico en las fuerzas armadas de USA para alcanzar una superioridad competitiva.
  - Experimentación en ejercicios y operaciones y consideraciones sobre resultados en el diseño, la recolección de datos, el análisis y la diseminación.
  - Experimentación con capacidades y amenazas virtuales para explorar posibilidades de transformación de mediano y largo plazo.
  - Experimentación con prototipos que permitan la evolución de conceptos, tecnologías, procesos y organizaciones.
  - Experimentación con amenazas agresivas que incluyan capacidades asimétricas y permitan la posibilidad de alcanzar innovaciones tecnológicas de magnitud (breakthroughs) y operar en una variedad de ambientes.
  - Uso de “red teams”. Operando al nivel táctico operacional y estratégico.

- Adopción de procedimientos y revisiones que permitan capturar y compartir las lecciones aprendidas.

### **Rol de los Servicios en la Experimentación.**

Los esfuerzos de experimentación dirigidos por los Servicios deberán ser consistentes con la hoja de ruta diseñada para la transformación de cada Servicio y a la vez con los esfuerzos de conjuntos de experimentación diseñados por el Comando de Fuerzas Conjuntas (JFCOM). Todo este conjunto de componentes señalados para desarrollar experimentación conjunta está orientado con alta prioridad a generar los siguientes resultados:

- Estructuras de comando y control conjuntos de despliegue rápido que tengan acceso a una información global proveniente de centros de información en todo el mundo y que permitan mejorar el empleo de fuerzas en forma más sincronizada y sinérgica por parte de los Servicios.
- Contar con herramientas que permitan una obtención y diseminación oportuna de información específica de un tipo de misión que esté disponible para los Comandantes en todos los niveles.
- Herramientas que permitan una mayor integración de los esfuerzos de inteligencia, vigilancia y reconocimiento (ISR) y sus productos.

- Capacidades conjuntas que permitan despliegues simultáneos, empleo sinérgico de fuerzas y apoyo a las capacidades combativas de aire, tierra, mar y espacio.
- Recomendaciones para reasignar recursos para aliviar las tensiones que despiertan demandas competitivas.
- Mejorar los resultados de operaciones conjuntas en áreas urbanas y en ambientes de selva.

### **Infraestructura de Apoyo.**

Una experimentación y desarrollo de conceptos vigorosa y dinámica necesita ser apoyadas por una infraestructura coherente. Esta infraestructura incluye los siguientes elementos:

- Juegos de guerra. Los juegos de guerra pueden ayudar a los servicios y agencia a desarrollar y evaluar conceptos de futuro. Los servicios y agencias pueden combinar entre ellos y con la comunidad conjunta capacidades y conceptos de corto, mediano y largo plazo que examinen ideas claves o identifiquen vacíos o fallas conceptuales. Los juegos de guerra pueden también realizarse distribuyéndose entre todos los servicios y agencias y sus resultados pueden ser analizados de manera que se realice un proceso continuo de desarrollo y refinación de conceptos futuros.

- Modelos y simulación. Se necesita una nueva generación de modelos y simulación para apoyar el desarrollo de conceptos. Estos nuevos modelos y simulación deberían estimular la experimentación y el entrenamiento ligando muchos tipos de simulaciones desde modelos computacionales agregados y detallados hasta la simulación de componentes de variado tipo.
  
- Capacidad de entrenamiento conjunto nacional. Esta capacidad de entrenamiento conjunto proporcionará datos del mundo real de ejercicio y operaciones con la capacidad de realizar experimentos que evalúen nuevas doctrinas, tácticas, técnicas y procedimientos empleando fuerzas militares reales contra fuerzas opositoras profesionales en condiciones y escenarios de combate realistas. Las lecciones que se aprendan de estos ejercicios de entrenamiento conjunto y de sus experimentos será una fuente principal para generar nuevos conceptos operativos.
  
- Lecciones aprendidas. Las lecciones aprendidas de las misiones operacionales debieran ser captadas, analizadas e incorporadas al proceso de desarrollo de conceptos y experimentación. Estos conocimientos permitirán al DoD ensayar nuevas tácticas técnicas y procedimientos al introducir todos estos conceptos a un proceso y ambiente de experimentación que permita determinar si estos conceptos tienen validez para ser aplicados como conceptos operativos reales. Lo que apruebe tener resultados positivos podrá ser incorporados institucionalmente a las fuerzas.

#### **Cuarto Pilar. Desarrollar Capacidades de Transformación.**

El DoD requiere desarrollar fuertes mecanismos para implementar resultados verificables a partir de los esfuerzos por desarrollar nuevos conceptos y su experimentación. Este proceso puede tomar algún tiempo. En tanto y en más corto plazo el DoD necesita desarrollar las capacidades necesarias para alcanzar los seis objetivos operacionales de la transformación descritos al comienzo de este análisis. Para alcanzar estos objetivos operacionales y en un rango mayor desarrollar las capacidades necesarias para alcanzar nuevos conceptos en operaciones futuras el Departamento debe diseñar hojas de ruta para las acciones de transformación, promover una investigación adecuada y test y sistemas de evaluación, además de transformar el entrenamiento conjunto y la educación. Asimismo debe continuar efectuando cambios organizacionales, cuando corresponda a nivel de los comandantes combatientes y de otras organizaciones militares.

Diseño de hojas de ruta de acciones de transformación. Este es el paso inicial para la transformación de los servicios y agencias del DoD y debe servir como una línea de base para evaluar las actividades de transformación del Departamento. La segunda generación de hojas de ruta debe enfocarse en las capacidades e indicadores de progreso alcanzado en los seis objetivos de transformación. Además las hojas de ruta de los Servicios contendrán un plan para adquirir las capacidades necesarias para apoyar las Operaciones

Conjuntas. A su vez existirá una hoja de ruta conjunta preparada por el Comando Conjunto (JFCOM) con los aportes de las agencias de defensa que entregue planes para construir las capacidades conjuntas necesarias en este tipo de operaciones.

Programas acelerados de investigación, desarrollo, ensayo y evaluación. Las hojas de ruta para los esfuerzos de transformación podrán enfrentar dificultades en su ejecución debido a la competencia con otras prioridades de los programas de defensa. Para asegurar la aprobación y ejecución de hojas de ruta en áreas críticas y para estimular diseños alternativos para adquirir las capacidades deseadas en forma más eficiente y efectiva aunque sea a costa de un mayor riesgo técnico el DoD está iniciando diversos programas de investigación, desarrollo, ensayo y evaluación. Algunos de estos programas son:

### **Programas de Iniciativas de Transformación.**

Una de las claves para alcanzar los objetivos de transformación del DoD es incorporar a los comandantes combatientes en el proceso de experimentación en diversos ambientes operacionales. De acuerdo con esto el llamado Programa de Iniciativas de Transformación se está desarrollando de forma que permita a estos comandantes diseñar e implementar diversas iniciativas de transformación que apoyen nuevas oportunidades de cambio.

Se espera que este Programa reforzará la capacidad de los comandantes de adquirir iniciativas conjuntas de transformación con un alto potencial de costo/beneficio. Se espera que estas iniciativas presenten nuevas oportunidades para desarrollar operaciones conjuntas y nuevas tecnologías en contingencias, ejercicios y experimentos.

### **Programa de Adquisiciones Conjuntas Rápidas.**

La transformación de la gestión del DoD comprende una reducción del tiempo empleado en cada ciclo de adquisición de materiales. El programa de adquisición conjunta rápida está administrado por el comando conjunto (JFCOM) en el DoD. Este programa está destinado a acelerar la implementación y ejecución de proyectos empleando nuevas pero probadas tecnologías y materiales que satisfagan las necesidades inmediatas de los combatientes. Su propósito es servir como un puente de financiamiento desde un programa experimental o de demostración de tecnología avanzada a un programa standard financiado por una agencia de defensa u otro actor en el DoD.

### **Transformación del Entrenamiento.**

La superioridad militar de las fuerzas de USA hoy en día se debe en gran parte al modo en que se entrenan estas fuerzas. El régimen de entrenamiento militar riguroso y realista proporciona a las fuerzas grandes ventajas en el campo de batalla. Este tipo de entrenamiento permite al combatiente maximizar el potencial de tecnologías más avanzadas aumentando así las diferencias entre USA y sus adversarios. Pero para mantener esta superioridad en el futuro se señala que la transformación del entrenamiento debe ser paralela e igualmente fuerte como en otras áreas de esfuerzo de transformación en el DoD.

### **Transformación de la Educación Conjunta.**

Para crear una cultura propicia a la transformación se afirma que es fundamental una educación conjunta basada en líderes que se sienten en disposición y están de acuerdo con estos cambios. Para alcanzar esta nueva cultura se requiere un enfoque de revisión fundamental dirigido a una educación profesional militar conjunta. La educación conjunta debe preparar los líderes capaces de conducir operaciones en forma coherente con un esfuerzo común y desarrollar su pensamiento con este fundamento en ambientes de incertidumbre.

### **Transformación de organizaciones.**

El cambio organizacional es fundamental en los esfuerzos de transformación militar. Al respecto se da el ejemplo de cambios recientes en las misiones y en las áreas geográficas bajo la responsabilidad de comandantes combatientes seleccionados así como la creación de un nuevo comando de combate. Estos cambios se han considerado cuidadosamente para diseñar nuevas y emergentes capacidades de las fuerzas y en respuesta a las cambiantes condiciones operacionales y estratégicas en el que operan las fuerzas. Algunos ejemplos son:

- Se creó el Comando Norte de USA para defender el territorio continental y proporcionar ayuda militar a las autoridades civiles.
- El Comando Conjunto se concentrará en la transformación de las fuerzas militares de USA. Sus responsabilidades geográficas actuales fueron trasladadas al Comando Norte y al Comando Europeo de USA.
- La fusión del Comando Espacial y del Comando Estratégico de USA dio paso a un Comando Estratégico de mayor tamaño. De esta forma a sus misiones y responsabilidades tradicionales se han añadido nuevas misiones del tipo Ataque Global, Misiles de Defensa y Operaciones de Información.
- La expansión del rol del Comando de Operaciones Especiales de USA cubriendo la guerra global contra el terrorismo es parte de este cambio organizacional. Este esfuerzo está dirigido por el propio Secretario de Defensa de USA. Un comentario final de esta transformación

organizacional es que luego de estas etapas de grandes cambios ahora deberán seguir transformaciones organizacionales a nivel de unidades más pequeñas.

### **Algunas Perspectivas y Críticas.**

Como se ha señalado en esta revisión de la RMA fueron los militares soviéticos quienes, a comienzos de la década de los 80' advirtieron a su liderazgo político de que había una nueva revolución tecnológica militar en marcha. Esta formulación era producto de su conocimiento del avance tecnológico de USA que abría un amplio margen para una superioridad americana en el uso de armas convencionales. En particular los soviéticos señalaban su preocupación por el desarrollo de la capacidad de USA para reconocer y atacar blancos a grandes distancias. Esta posición de una nueva perspectiva en la guerra convencional se intensificaba con la preocupación soviética y su temor ante la Iniciativa Estratégica de Defensa (SDI) lanzada por el Presidente Reagan hacia 1986. De este modo, la SDI de Reagan era vista como una costosa nueva carrera espacial en la que USA tenía grandes ventajas en el uso de sensores, computadores de alta velocidad, satélites y otra cantidad de elementos que le daban una ventaja formidable. Sin embargo, hay que anotar que esta formulación de la Revolución de Asuntos Militares (RMA) por los rusos no concentró tanta atención en la década de

los 80' como lo hizo a partir de la década siguiente. Se comenta que esto puede tener diversas explicaciones provenientes de la manera de pensar de los planificadores militares en plena época de Guerra Fría concentrándose en

el “deterrence” nuclear por una parte y en el campo de uso de armas y fuerzas convencionales donde el pensamiento estratégico estaba concentrado en un escenario de Europa central alrededor de las fuerzas de la OTAN y el Pacto de Varsovia. Como se sabe, en este potencial escenario de enfrentamiento ambas alianzas poseían formidables capacidades convencionales del tipo que se había empleado en las guerras pasadas y sin una variación importante en el modo de conducir un conflicto mayor.

En todo caso a fines de la década de los 80’ la investigación y el desarrollo tecnológico de USA había dado pasos muy importantes con el desarrollo, entre otras, de las llamadas “armas inteligentes” junto con otros desarrollos tecnológicos relativos a sensores, tecnología de información, vigilancia satélital, etc.

Sin embargo, mientras USA desarrollaba y proponía importantes mejoras tecnológicas en la capacidad convencional de fuerzas propias y amigas muchos gobiernos europeos miraban con cierta suspicacia las proposiciones y cambios tecnológicos militares de USA por el serio impacto del alto costo de estos nuevos sistemas sobre el presupuesto de defensa y la sospecha de que estos progresos tecnológicos representaban buenos negocios para la industria de la defensa de USA. En suma, predominaba una tendencia al *stato-quo* ante la adopción de nuevas tecnologías de uso militar

convencional. Fue así como el movimiento mundial contra el empleo de armas nucleares a fines de los 70’y comienzo de los 80’ disminuyó la dependencia y el riesgo nuclear dando paso a una estrategia alternativa de

desarrollo de una capacidad convencional de ataque a larga distancia y de alta precisión a través de nuevas misiones tácticas. Así en 1982 en una reunión de la OTAN en Bonn el Secretario de Defensa de USA Caspar Weinberger propuso una Iniciativa de Tecnologías Emergentes que despertó preocupación a sus aliados europeos que se enfrascaron en una discusión sobre el costo de estas proposiciones y las exiguas disponibilidades presupuestarias de Defensa en varios países europeos.

Es interesante observar que mientras el elevado gasto de investigación y desarrollo del DoD producía innovaciones y nuevos sistemas de armas muchos de los planificadores militares tenían diferentes puntos de vista sobre los cambios que estaban ocurriendo y sobre la visión de los desafíos futuros. Así se señala que se mantenía un DoD concentrado en la gestión de adquisiciones y tareas que habían caído en un cierto manejo burocrático. El concepto estratégico seguía concentrado en “guerras de atrición” orientadas a destruir el enemigo en enfrentamientos totales. Sin embargo predominó de parte de la conducción de los líderes del DoD una fuerte revisión de los principios estratégicos por una parte y un continuo apoyo y explotación de las fortalezas tecnológicas de USA.

Este movimiento de reforma y cambio estratégico se hacia mientras persistía el escenario de enfrentamiento OTAN – Pacto de Varsovia y los criticos del cambio tecnológico señalaban que era una idea inocente creer que la

estrategia podría conducir la tecnología si bien reconocían que descansar sólo en el progreso tecnológico en forma aislada podía ir en detrimento de las fuerzas de USA. Es digno de anotarse que en la década de los 80' había voces y opiniones que negaban que los progresos y desarrollos tecnológicos convencionales favorecieran la Defensa. Los recursos del presupuesto de Defensa de USA en ese momento, destinados a la adquisición de equipos buscaban recortar los sistemas a adquirir y el resto del gasto militar tendía a reducir el nivel de combatientes. En esta visión las adquisiciones de nuevos sistemas de armas se veían por algunos críticos como de alto costo de mantención, poco confiables y con demandas logísticas elevadas lo que convertía el proceso de adquisiciones (procurement) en un intrincado mecanismo sin visos de poderlo simplificar o acelerar. Al respecto, se llegaba a decir o a pensar que a pesar de potencialidades teóricas de destrucción de los nuevos sistemas, en la práctica se obtenían menos resultados que los esperados debido a que los problemas derivados del clima, el terreno, el polvo, el humo y las tácticas del adversario creaban serios problemas a la identificación confiable de los blancos. Se llegaba a decir que el uso de estos nuevos sistemas y armas “hacían más compleja la vida del soldado”.

Hay que recordar que incluso los planes de operación de la OTAN a comienzos de los 80' contemplaban ataques en profundidad a la retaguardia enemiga contra blancos fijos como puentes y aeropuertos y en estos

objetivos se confiaba en las nuevas tecnologías. Sin embargo se era muy escéptico en cuanto a la capacidad de detectar y atacar con precisión blancos en movimiento.

### **El Impacto de la Guerra del Golfo.**

Hasta 1990 no existía evidencia suficiente de como se comportaría el uso de las nuevas tecnologías militares en la práctica. En ese momento se tenían algunas indicaciones de lo que podían lograr las “armas inteligentes” y otras tecnologías a través de los ejemplos de su uso por Israel en la guerra contra el Líbano en 1982 y en la campaña de Las Malvinas Falklands ese mismo año. En ese tiempo las fuerzas de USA enfrentaron problemas como los rehenes en Irán; francotiradores en Grenada; autobombas en Líbano y tráfico de drogas en Panamá que no requerían gran empleo de fuerzas ni uso de sistemas de armas complejos. El colapso de la Unión Soviética en 1989 creó un nuevo escenario mundial en que USA permaneció como la única super potencia mundial. Estos formidables cambios marcados por la reducción del peligro nuclear y por el termino del enfrentamiento en Europa Central iniciaron una tendencia mundial a la reducción de los potenciales bélicos y fuerzas militares en las grandes potencias que se reflejaron en grandes

recortes de los presupuestos de Defensa. En forma coetánea, se abrió una oportunidad para una reflexión y planificación nueva y fresca sobre el futuro de los conflictos armados y las nuevas amenazas, aunque sin prever para nada la peligrosidad del terrorismo. Así las cosas, en 1990 Irak invadió

Kuwait y se produjo la Guerra del Golfo. Hay quienes afirman que la Guerra del Golfo transformó las percepciones de USA sobre su poderío militar. Hasta ese momento, la sombra de Vietnam había disminuido la confianza en la capacidad de las fuerzas armadas de USA en combatir y ganar una guerra. Incluso en vísperas de la llamada Operación Tormenta del Desierto se tenía la convicción de que las fuerzas de la coalición podrían sufrir grandes pérdidas al enfrentar a las defensas iraquíes precisamente porque todo el plan de ataque de USA y sus aliados se basaba en el empleo de tecnología militar avanzada. Incluso se señalaba que la arena del desierto podía interferir y dañar los delicados equipos y alterar los indicadores del campo de batalla de manera que el fuego sobre el bando amigo podía ser un gran riesgo. El gran número de bajas que se estimó como muy probable tenía una imagen muy negativa a nivel político y social en USA.

El resultado de este conflicto es conocido. Las nuevas tecnologías militares fueron empleadas exitosamente y se produjo una verdadera revolución de expectativas y nueva confianza pública en la capacidad militar de USA que apareció como una potencia militar imbatible.

A pesar de las observaciones críticas de los resultados de la Guerra del Golfo como una “guerra en un escenario ideal y contra un enemigo ideal” la prueba de fuego de las nuevas tecnologías militares fue aprobada y desde entonces tiene un sostenido apoyo público. Esto fue el resultado de las imágenes del Golfo en que se apreciaba el impacto de bombas “inteligentes” penetrando

un centro de comando o el impacto de un proyectil crucero Tomahawk disparado a 1000 kms. de distancia e impactando en su blanco. A su vez la

Guerra del Golfo ha recibido el calificativo de la “primera guerra de información y comunicaciones” y la “primera guerra del espacio”. En lo relativo a las comunicaciones, el desempeño tecnológico fue impresionante y en la guerra espacial, aunque no se emplearon armas, se obtuvo información de 64 satélites individuales de 23 tipos diferentes con usos de comunicaciones, meteorología e imágenes que permitían una información muy completa de inteligencia, ubicación de unidades y comunicación con los comandantes. Estos sistemas basados en el espacio identificaron blancos, ubicaron fuerzas amigas y enemigas ayudaron a seleccionar el sistema de armas mejor ubicado para atacar, entregaron las órdenes de ataque y aún corrigieron la dirección de los misiles. Este conflicto empleó muchos terminales de satélites y se dio el caso del primer uso en un conflicto de los sistemas llamados GPS o Sistemas de Posicionamiento Global que han tenido tanto éxito en su empleo tanto militar como civil en la actualidad. En suma este empleo tecnológico incluida la guerra electrónica dejó a los iraquíes en una posición de ciegos, sordos y mudos.

Sin embargo no todo resultó exitoso. En verdad en el Golfo se lanzaron más bombas “necias” que del tipo “inteligente” y, a diferencia de lo que se creyó por todo el mundo, en ese momento el sistema de proyectiles defensivos “Patriot” fallaron frente al uso de proyectiles ofensivos “necios” como eran

los “Scud” rusos. Además no siempre se obtuvo éxito en encontrar los blancos ni en destruirlos y el llamado “daño colateral” no siempre se pudo evitar. Por último las comunicaciones y sensores de datos que forman la esencia de la guerra informativa no siempre funcionó bien.

A pesar de todo, parece evidente que la revolución tecnológica militar logró un gran impulso en el pensamiento estratégico militar de USA como se reveló posteriormente en el conflicto en Afganistán e Irak. Esto llevó a decir por algunos que “la Guerra del Golfo desencadenó la RMA”. Al respecto el Secretario de Defensa de USA Richard Cheney en la época habló de una revolución en la manera de combatir un conflicto cuyas posibilidades se habían “demostrado dramáticamente” en la Guerra del Golfo. Con posterioridad un estudio académico concluyó que aunque la revolución de la RMA estaba en desarrollo la Guerra del Golfo había delineado sus alcances con claridad.

Así las cosas, mirando a la década del 80’ en que se acuña la RMA como termino-estratégico militar y luego la experiencia de la Guerra del Golfo se constata que la expresión “Revolución de Asuntos Militares RMA” comenzó a tener fuerza al mismo tiempo que admitía distintas acepciones y aun contenidos según que actor o sector usaba esta terminología emergente. Así, para muchos predominaba un contenido de “cambio tecnológico e

innovación” mientras otros ampliaban la RMA más allá de lo tecnológico e incluían conceptos organizacionales novedosos. Estos últimos conceptos alcanzaban incluso al grado de desarrollo de nueva doctrina en los asuntos militares. Pero todavía quedaba la experiencia de los conflictos en

Afganistán e Irak que dieron nuevo impulso y exposición favorables a los conceptos emanados de la RMA y en la actualidad siguen siendo empleados de distintas formas y grados en el escenario vigente de transformación militar que es el cambio estratégico principal en la política de defensa de USA.

### **Otras consideraciones sobre la RMA.**

La concentración de contenidos de la RMA en la ventaja tecnológica militar y sus constantes innovaciones no impide que todo este potencial de material ofensivo o defensivo sufra el escrutinio de como puede operar una fuerza en distintos teatros y condiciones de combate. Un caso destacado es el que representa los problemas de un escenario de operación urbana. La operación militar en ciudades es muy compleja tanto en lo relativo a los blancos como a las maniobras. En documentos oficiales de USA se señala que el combate en zonas urbanas enfrenta la dificultad de la madeja de calles, la complejidad de los edificios, las construcciones de altura y subterráneas y la población atrapada, todo lo cual demanda un empleo creciente y masivo de fuerzas terrestres, complica el uso de sistemas de armas y puede llegar a frenar las operaciones. A esto se añade la consideración y deber de no comprometer a los no-combatientes, proteger estructuras vitales y manejarse con los líderes civiles todo lo cual tensiona el empleo de fuerza en

ambientes urbanos. Esto ha llevado muchas veces a que las fuerzas de USA en el caso de conflictos asimétricos prefieran dejar estos escenarios urbanos como una responsabilidad de los aliados locales.

Se destaca que el ambiente y características del teatro de operaciones militares determinará el uso y la ventaja de las nuevas tecnologías. Así, si se trata de escenarios con blancos fijos y grandes plataformas que son detectables aunque se desplacen en el terreno serán vulnerables a sistemas de armas de ataque lanzados desde puntos fijos y desde distancias variables pero estos equipos no serán posible de utilizar en contra de sistemas pequeños y pasivos que no despiertan atención militar y pueden emerger y atacar desde cualquier posición. Esto ha llevado a decir que la infiltración a través del mar llegará a ser más difícil que la infiltración terrestre y que las operaciones en ciudades y selvas será más problemática que en los desiertos.

Otro punto debatido es el relativo a si las nuevas tecnologías favorecen las acciones defensivas. Esta interrogante se responde positivamente cuando se trata de defender una porción de territorio contra un invasor pero se hace menos aparente en el caso que en la defensa de territorio haya que desplazar fuerzas para prevenir un ataque inminente, liberar un territorio capturado o auxiliar a fuerzas aliadas. En estos casos se dice que la selección de equipos defensivos u ofensivos es muy compleja y puede conducir a errores.

Otro problema conocido del empleo de fuerzas y de equipos es el de la movilización y transporte hacia el área de operaciones. Desde la época del Pacto de Varsovia la rapidez de movilización y transporte de personal y material fue siempre reconocida como una de las mayores dificultades para responder a una agresión del Este. Se partía de la premisa que el apoyo

logístico en “tiempo real” a áreas de conflicto era y es imposible pero aún hoy el progreso que se ha alcanzado en materia de transporte al campo de batalla es muy inferior a la rapidez demostrada en la habilidad para montar operaciones una vez que se está en el área elegida. Esto ha llevado a otorgar más confianza en el uso de misiles de largo alcance así como de aviones salidos de sus bases habituales y en la llamada “fuerza de tarea naval” por su capacidad de desplazamiento de grupos de portaviones dotados de aviones de largo alcance. Por lo demás, los sistemas de armas fijos en terreno no sustituyen las tropas que operarán en tierra y en todo caso estos sistemas corren riesgos de deterioro en el periodo de embarque y desembarque debido a su gran tamaño y peso. Pero también el desplegar personal y equipo en un área de combate conlleva a peligros emanados de las defensas locales especialmente si estas maniobras demoran tiempos útiles para que el enemigo les impida la entrada, ejecute el minado de tierra y mar o instale defensa aéreas. Todo lo anterior se refiere a las condiciones y factores que no son relativos a la ventaja tecnológica misma de sistemas de armas avanzados sino a otros factores que limitan la superioridad de la fuerza militar convencional de USA y que corresponden a factores locales que, bien usados por el adversario, pueden ocasionar desagradables sorpresas.

### **La amenaza de destrucción masiva.**

En el último tiempo el argumento del uso de armas de destrucción masiva (WMD) por fuerzas hostiles en el caso de operaciones ofensivas por parte de

USA o sus aliados ha predominado en la discusión militar. Al respecto es bien conocida la posición de Washington de controlar y eliminar el uso de artefactos nucleares como una opción en el modo de enfrentar conflictos o hacer pesar este factor en la política internacional. En verdad hasta ahora las discusiones sobre la RMA casi no contienen referencia al tema de uso de WMD. Desde el termino de la Guerra Fría se ha usado y mantenido el “deterrence” nuclear contra la Unión Soviética pero no hay evidencia de su empleo o amenaza contra otros enemigos como es el caso de Irán o Corea del Norte.

Sin embargo el riesgo de una adquisición de tecnología nuclear o de la capacidad de fabricar un artefacto de este tipo a partir de “escapes” o acuerdos con Rusia y el impacto de las revelaciones recientes sobre los programas nucleares en Corea del Norte e Irán han revivido la preocupación de los encargados de la seguridad en el Oeste. Esto para no añadir el riesgo representado por el uso de una “bomba sucia” que no requiere tanta sofisticación tecnológica y que puede ser transportada por un solo hombre sin llamar la atención. El riesgo del programa nuclear de Irak y su influencia en la guerra contra ese país es suficientemente conocido con su resultado negativo en lo referente a hallazgos de este tipo de armas en ese país después de la invasión. Pero la preocupación por el uso de este tipo de armas se

concentra no sólo en los países señalados sino que en la peligrosidad de la acción de grupos terroristas. La seguridad y porosidad del sistema de control de armas de todo tipo especialmente las biológicas, químicas y nucleares está puesta a prueba hoy día cuando se trata no sólo de la conducta de

actores estatales sino que de actores sin respaldo de un Estado. El riesgo de adquirir armas nucleares por grupos terroristas se aprecia mas lejano dada la complejidad técnica de su manejo pero en el caso de las armas químicas y biológicas el acceso por estos grupos puede ser posible en cualquier momento. Es sabida la gran mortalidad representada por el antrax que en su forma de esporas o polvo puede matar gran cantidad de personas y contra esta acción letal no existe protección segura. En la identificación de grupos de mas peligrosidad que pueden tratar de adquirir WMD se anota en primer lugar la acción de terroristas pero también hay que registrar a organizaciones criminales, grupos religiosos extremistas, grupos étnicos separatistas y otros.

Cualquiera de estas personas o grupos pueden llegar a tener oportunidades de cometer ataques violentos y trastornar actividades causando pánico y destrucción en cualquier parte del mundo.

Frente a esta amenaza de uso de WMD, USA ha acentuado su actividad de información y control de estos riesgos potenciales. En todo caso, el formidable arsenal nuclear de ese país ofrece un manto de seguridad entre sus aliados frente a un riesgo de este tipo pero no asegura ningún control frente a armas biológicas o químicas salvo la autorización expresa para usar armas nucleares si algún enemigo llega a atacar el país usando armas

químicas o biológicas. Esto último en la práctica no pasa de ser una declaración sin mucho asidero real a pesar de que Irak ha señalado que fue disuadido de usar armas químicas en la Guerra del Golfo por la posible respuesta con un ataque nuclear de parte de USA y aún de Israel. Al

respecto, lo más probable es que, ante cualquier ataque biológico o químico, los gobiernos de Occidente apoyen una respuesta militar convencional en vez de contratacar con artefactos nucleares.

En todo caso la experiencia de la guerra en Irak al no demostrar la existencia de WMD puso más bien de relieve la insuficiencia e imprecisión tanto de los controles de los inspectores de las Naciones Unidas y de la Comisión Atómica como de la inteligencia e información recolectada en la etapa previa del conflicto lo que ha dado más de un dolor de cabeza a los líderes de USA, Inglaterra y otros países. En todo caso el peligro de las WMD existe y continúa preocupando y los esfuerzos de su control a través de vacunas y otras medidas preventivas es una obligación permanente y creciente de los países que enfrentan más riesgos.

### **Guerra de Información.**

Como se ha señalado, el amplio campo y el avance tecnológico de la información ha convertido a esta actividad en una nueva área de posible

conflicto. Este nuevo campo de combate ha alcanzado un estatus formal a nivel del DoD que señala a las Operaciones de Información como “aquellas acciones militares que permiten, refuerzan y protegen la capacidad de las fuerzas amigas para recoger, procesar y analizar la información necesaria para obtener una ventaja en las operaciones militares. Las Operaciones de Información incluyen interacciones con los sistemas globales de información así como con acciones de acceso o de negación de la información del adversario”.

Las Operaciones Militares en el campo de la Información ofrecen importantes capacidades a los comandantes operativos. Esto comprende tanto el aportar información de satélites militares y civiles entregando información de meteorología y datos al día de ubicación de defensas aéreas como también sacar información de una variedad de fuentes de datos que permiten obtener una visión de las partes más relevantes de un campo de batalla. Como se ha dicho, hoy se habla de un Ambiente Global de Información para designar una red de cobertura mundial con accesos a fuentes de información, archivos y usuarios. Al hablar de esta red de interconexión mundial se comprende que se accede a datos cuyo alcance excede las fronteras nacionales y las institucionales y que incluso tienden a borrar las diferencias entre el acceso y el uso de estos sistemas por parte de los sectores civiles y militares.

A los fines de este estudio la revolución de las tecnologías de la información (IT) justifica su inclusión en una revisión de los alcances de la RMA. Sin embargo como en tantas áreas de los asuntos militares el progreso tecnológico de la información en el caso de conflicto permite, por una parte,

una gran contribución a la eficiencia de las acciones bélicas, a discriminar y seleccionar el uso de armas y a reducir las bajas. Por otra parte, muchas de estas nuevas oportunidades dan margen a nuevas vulnerabilidades que son un campo de explotación para potenciales adversarios.

Al comenzar esta revisión de la información como un nuevo campo de conflicto hay que evitar el peligro de exagerar el alcance y posibilidades de la revolución de la IT en los asuntos militares precisando en particular cual es el verdadero aporte o efecto que la información puede hacer por si sola. Esto quiere decir que por si misma la información militar no puede potenciar, destruir, proteger ni mover fuerzas en combate pero si puede entregar un apoyo vital para todas estas funciones. Los comandantes siempre han protegido su capacidad de obtener, transmitir y aplicar información vital para atacar al enemigo. De allí que el debate sobre la contribución de la información en un conflicto se hace siguiendo y respetando las áreas de acción bien establecidas y vitales como es el caso de comando y control, inteligencia, guerra psicológica, etc.

En este debate sobre las potencialidades de la información militar ha surgido la cuestión si el rol principal de esta sería predominantemente de carácter táctico como apoyo general a las fuerzas o, más bien, de tipo estratégico o sea que el factor información pudiera ser decisivo para un resultado exitoso

al entregar datos que permitan ataques directos en los puntos más sensibles del adversario. La verdad que estas dos apreciaciones persisten sin tener una evidencia suficiente para apoyar más una interpretación de arma táctica o arma estratégica.

### **Alcances y magnitudes de la Información.**

El desarrollo de las IT ha convertido a la información en un recurso abundante y que se ha hecho alcanzable a mayor población a medida que evolucionan estas tecnologías. Esto ha llevado a que mucha información militar se puede obtener de sistemas comerciales civiles que comparten sus datos sin distinguir amigos y enemigos. Esta diseminación inmediata de datos alcanza no solo a los sistemas de televisión por cable sino que, en el caso de la tecnología GPS, hoy en día los usuarios de estos sistemas por canales comerciales exceden ampliamente a los usuarios militares, aunque no con la misma precisión de datos. Hay que anotar que han existido intentos de limitar el acceso a estos servicios tan abiertos pero estos esfuerzos se han visto derrotados por las reglas comerciales y las garantías contractuales exigidas para el desarrollo de estos sistemas especialmente en

un ámbito de competencia comercial. Pese a esto se dispone de algunos sistemas de información protegida por sistemas de claves que entregan cierta seguridad en lo referente a información financiera, sistemas y servicios de

información protegida que se están desarrollando en otros campos de comunicaciones.

Sin embargo, el caso de las imágenes satelitales de gran poder de resolución los esfuerzos por restringir su acceso se han visto frenados por la demanda del público usuario de tener servicio ininterrumpido y no restringido por consideraciones de seguridad nacional. Se señala además que en el caso de los satélites de USA si su acceso está restringido por diferentes cláusulas, un usuario puede recurrir a los servicios de satélites de Francia, India y Rusia. Al respecto se recuerda que desde 1996 los lanzamientos satelitales comerciales superaron al número de lanzamientos satelitales gubernamentales. Incluso se señala el caso ocurrido en 1997 de la primera experiencia de un “satélite espía” civil que fue puesto en órbita por una compañía de USA montándolo en un cohete ruso y cuyos servicios se ofrecían con un poder de resolución similar a los satélites militares. De allí que hoy día predomine un mercado de imágenes satelitales con pocas restricciones a pesar que el Gobierno de USA mantiene el derecho a investigar a los clientes extranjeros a la vez que puede apagar las cámaras satelitales en caso de conflicto.

A pesar de todo este avance tecnológico las imágenes satelitales todavía presentan problemas de recolección e interpretación pero los imágenes de los sistemas GPS se han multiplicado a través de su incorporación en radios,

teléfonos celulares y computadores personales creando una verdadera red portátil y accesible de bajo costo.

A su vez, la mejora técnica de la calidad de los servicios de información civil ha sido tan impresionante que muchas organizaciones militares las usan en su trabajo diario. Se recuerda el caso de los comandantes ingleses que usan la información de la BBC de Londres para muchas informaciones por su mayor rapidez de diseminación por sobre la transmisión a través de las jerarquías militares. Se llega a decir que hasta el 90% del tráfico de información del Pentágono descansa en sistemas de telecomunicaciones comerciales.

Sin embargo, a pesar de todas estas posibilidades y restricciones en el uso de información espacial se ha demostrado que una fuerza enemiga puede desarrollar una red de comunicaciones muy útil e importante usando teléfonos celulares que no puedan ser detectado o interferidos con facilidad.

### **Dependencia e Interferencia de Información.**

Uno de los principios del pensamiento estratégico es evitar el punto en que un factor de combate alcanza el punto de dependencia, esto es el momento en que ese factor, como puede ser la información, resulta crítico para las operaciones. Dicho en otras palabras la “dependencia” rápidamente se convierte en “vulnerabilidad” y de allí se puede convertir en un objetivo bélico. Esto lleva que junto con el progreso de las IT el desarrollo de la información levanta los esfuerzos de interferirla, manipularla o simplemente destruirla.

En el caso de los satélites que son artefactos sin armas y fácilmente detectables se conoce su rol esencial para propósitos de navegación, inteligencia meteorología y comunicaciones el desarrollo de toda esta infraestructura militar colocada en el espacio ha despertado el temor, de acuerdo a la lógica militar, de desarrollar sistemas anti-satélitales que los puedan destruir. Sin embargo este tipo de sistema capaz de localizar y destruir un satélite es muy improbable que llegue a ser empleado por la cadena de efectos que un hecho así produciría. Nadie duda que destruir un satélite en el espacio es un acto de hostilidad abierta que fácilmente puede escalar hasta una crisis por ello se hace muy poco confiable el empleo de estos sistemas que enfrentan, a su vez, muy altos márgenes de error.

En este punto se tiene que recordar el gran debate en la época del Presidente Ronald Reagan sobre lo que él llamó la Iniciativa de Defensa Espacial (SDI)

que causó tanto revuelo internacional pero que nunca alcanzó a convencer a los expertos del Pentágono que sus ventajas superaban a los riesgos y altos costos que se fueron detectando.

De allí que hoy se crea que, dada la complejidad y alto costo del desarrollo de sistemas anti-satélites pocos países podrán tener acceso a este tipo de armas espaciales. Los sistemas anti-satélites desarrollados por los soviéticos sólo llegaron a amenazar satélites en órbitas inferiores a 5.000 kms. Pero es muy difícil alcanzar sistemas satelitales de órbitas a 20.000 kms. de altitud que es donde se encuentran los satélites de comunicaciones y de alerta temprana.

La frase dicha hace 40 años atrás que USA “peleará desde el espacio y hacia el espacio” hoy no goza de mucha credibilidad por sus grandes riesgos. Sin embargo, de tiempo en tiempo se reviven teorías y proposiciones de “guerras espaciales”. La evolución de estas visiones ha vuelto a fijar la atención en el uso de los proyectiles balísticos intercontinentales que tienen la ventaja sobre las armas espaciales de un tiempo de respuesta y de un costo de preparación mucho menor que los artefactos en el espacio

**La Información Cibernética como componente estratégico en el conflicto.**

En esta parte del análisis del RMA se revisa el campo de la cibernética con su inmenso progreso pero, a la vez, con la creciente sofisticación y reiteración de ataques de hackers o de inventores de virus. Se conoce que los sistemas de comunicación y de información cibernética del Pentágono son un blanco preferido y continuo de ataques provenientes de hackers para quienes penetrar estos sistemas del DoD tiene una especial atracción. Si bien el caso de hackers o de inventores de virus puede tener diversos propósitos es factible pensar que otros grupos puedan tener propósitos de alteración o confusión usando estas técnicas en el caso de una guerra. Así, se puede intentar desorientar o interrumpir los sistemas de defensa aérea, desviar el curso de misiles de largo alcance o cortar las comunicaciones de los comandantes y alterar sus sistemas de control de sus sistemas de armas causando graves trastornos en el campo de batalla. Este potencial de la llamada “guerra cibernética” es un factor que causa preocupación en todos los encargados de la seguridad y la defensa.

La alteración de la información no sólo compromete el área militar sino puede ser usada como arma estratégica para dañar el potencial de una Nación procurando por ejemplo el colapso del sistema bancario, la pérdida del control de tráfico aéreo o el corte de la transmisión de la energía. Otras posibilidades de ataques cibernéticos pueden ser la interferencia o manipulación de los mensajes con fines de engaño o confusión. Con este carácter de intrusión psicológica se pueden imaginar muchas otras posibilidades de interferencia de los sistemas de información en áreas sensibles o de seguridad de un país. Sin embargo se ha avanzado en forma paralela en reducir el riesgo de ataques cibernéticos a través de sistemas de

detección y eliminación de virus, control de acceso y mal uso y otras medidas de prevención que han disminuido este tipo de riesgos.

En todo caso hasta ahora no se ha demostrado que todo el potencial teórico de ataque cibernético este exento de errores y fallas en su ejecución y de allí que las llamadas “operaciones de guerra de información” son miradas con mucha prevención y con plena conciencia de los riesgos involucrados. Pero aún en el caso de una campaña de ataque cibernético exitoso se duda que el atacado tuviese una respuesta equivalente. En otras palabras, a la hora de medir ventajas y beneficios en un objetivo de destrucción o desarme de una instalación militar, el ataque electrónico o cibernético se debe pesar contra los resultados de usar armas mas directas y violentas. Generalmente, se cree que se preferirá el uso de armas más directas. De allí que se tiene una cierta resistencia a confiar demasiado o en forma exclusiva en operaciones de “guerra de información”.

Con todos estos antecedentes, la situación que se presenta es que los países desarrollados están menos sujetos hoy en día a este tipo de ataques que países con menos desarrollo que son más vulnerables por su insuficiente capacidad tecnológica de control y respuesta ante un ataque cibernético. De allí que la situación prevaleciente entre los estamentos militares es que hay que vivir sabiendo la existencia y las posibilidades de ataques a los sistemas de información abierta y no estar ansioso por construir una capacidad de rechazo. Esto obliga a todos los comandantes a ajustarse a todas las características de los medios de comunicación. Sin embargo en USA se señala que las amenazas de guerra de información pueden presentar los mas grandes desafíos a la hora de diseñar el ambiente de seguridad de ese país en

los años futuros. Al respecto se señala que la amenaza cibernética es difusa y difícil de localizar y que un concepto como el “control del espacio cibernético” es una mera formulación de deseos de proteger el sector amigo mientras se niega la información al enemigo, pero sin tener una gran precisión en estas formulaciones ni en la capacidad de ejecución de las mismas.

Por esta y muchas otras razones se ha ido decantando una opinión prevaleciente cual es que la “guerra de información cibernética” ha traspasado la frontera de lo plausible. En suma, se señala que abundan las medidas que puedan cegar, paralizar o confundir al adversario pero aun no se cuenta con un panorama claro de posibles efectos y consecuencias no previstas que podrían anular las ventajas y aun tener efectos contraproducentes al objetivo deseado. Así la revolución tecnológica de la información y las telecomunicaciones como parte de la RMA tiene, por así decirlo un doble rostro. Por un lado, tiene una capacidad creciente de acceder a información oportuna y pertinente y la capacidad de comunicarla directa e instantáneamente a través de toda la cadena de mando. Por otro lado persisten las posibilidades de mala interpretación, errores y engaños en la información recibida lo que puede ser de gran impacto negativo si acaso se tiene una gran dependencia de estas fuentes y canales de información.

**Corporación de Estudios Estratégicos (CEES) Septiembre 2005.**