

Fue a partir de estos desarrollos que aparecieron muchos de los sistemas que hoy día se asocian con una RMA convencional (no-nuclear) incluyendo progreso en tecnologías de propulsión, miniaturización, sistemas de guías de precisión y otros. Como se ha dicho, todos estos desarrollos se combinaron en la producción de los misiles cruceros de largo alcance reconocidos hoy como una de las más importantes innovaciones militares de los años 70'. Hay que recordar que estos misiles cruceros aparecieron con un amplio potencial ofensivo que borraba las líneas entre las armas de uso nuclear con las de uso convencional. Casi al mismo tiempo, ocurrió el desarrollo de toda una gama de innovaciones basadas en el espacio incluyendo la especialización de satélites orientados a la geodesia, meteorología y recolección de datos pero cuya aplicación principal ha sido su uso como instrumento de reconocimiento y espionaje. Así las cosas, el Presidente Reagan lanza en 1983 su llamada Iniciativa de Defensa Espacial (SDI) orientada a crear un sistema que protegiera como "escudo en el espacio" y capaz de interceptar ataques a USA con misiles balísticos. Este proyecto, que despertó gran agitación internacional entre USA y la Unión Soviética, estaba destinado según se decía a reducir la amenaza nuclear pero muchos piensan que sus efectos a largo plazo habrían sido un gran robustecimiento del desarrollo de nuevas tecnologías militares y espaciales que hubiesen permitido su empleo en acciones militares convencionales. En todo caso, la SDI no alcanzó más que el nivel de ensayos, no siempre exitosos.

Emergen Nuevas Tecnologías.

Las tecnologías desarrolladas como parte del esfuerzo de perfeccionar una estrategia nuclear menos apocalíptica tuvo como efecto un amplio campo de aplicaciones para su uso en operaciones militares convencionales. Así, los satélites fueron puestos en uso para fines de reconocimiento a comienzos de los años 60' y con fines comunicacionales en la guerra de Vietnam desde 1965. Los primeros computadores tácticos se emplearon en 1966 y los orígenes de Internet se remontan al proyecto ARPA del Pentágono a comienzos de los años 60'. El primer mensaje de correo electrónico fue enviado en 1972. Curiosamente, la primera demostración del potencial de los modernos misiles se atribuye al ataque de la Marina de Egipto sobre un buque israelí usando los misiles anti - buques del tipo **styx** en 1967. El caso del uso y apreciación del impacto potencial de las armas llamadas "inteligentes" provino de la Fuerza Aérea de USA en las últimas etapas de la guerra de Vietnam. Estos progresos tecnológicos se extendieron también a desarrollos que protegieran tanto blancos fijos como móviles los que se ensayaron con éxito en las armas de defensa anti - aérea y de tipo anti - tanque usadas en la guerra árabe - israelí en 1970. **Con estos datos se puede identificar a la década del 70' como la más productiva en innovaciones tecnológicas hoy asociadas con la RMA.** Esta lista incluye: sistemas de guías de precisión; de guías bajo control remoto; identificación de objetivos militares; mejoras en las municiones; guerra electrónica y comunicaciones; etc.

Este impresionante nuevo repertorio incluye toda una información sobre la letalidad atribuida a los nuevos sistemas de armas; al rango de distancia desde el cual estas armas pueden ser disparadas sin pérdida de precisión; a la calidad de la información tanto de los objetivos enemigos como de las fuerzas propias y de la velocidad con que todos estos nuevos elementos y sistemas pueden interactuar y comunicarse. Esto ha llevado a que las armas más modernas dependen cada vez más de sistemas electrónicos que permiten seguir y atacar blancos enemigos a la vez que impedir las mismas acciones de parte del enemigo.

Todas estas innovaciones tecnológicas llevaron a diversas formulaciones de los expertos sobre las nuevas posibilidades abiertas por estos cambios. Así, en 1974 un experto de gran prestigio de USA dio el siguiente testimonio frente al Congreso de ese país: “una impresionante serie de desarrollos tecnológicos nos ha colocado en el umbral de lo que se convertirá en una verdadera revolución en conflictos convencionales”.

Casi 10 años después, en 1985, otro connotado experto señaló con gran conocimiento: “estamos en medio de un periodo de cambio revolucionario de la tecnología de uso con nuestras fuerzas militares. En una o dos décadas, nuestras fuerzas serán transformadas radicalmente en sus doctrinas, modo de operación y capacidades. La revolución de asuntos militares está conducida por los mismos progresos tecnológicos que están haciendo abismantes cambios en el mundo civil. Estos avances incluyen principalmente desde la aplicación de electrónica de estado sólido (hoy chips) hasta computación, sensores, guías, comunicaciones y control de toda clase artefactos y maquinas”.

Como se aprecia, ya hace veinte años se percibía que el progreso tecnológico en todas las áreas mencionadas incluyendo los sistemas de comando y control convertían a la “guerra de información” como un elemento esencial en la conducción de futuros conflictos.

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.

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 *status-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 hacía mientras persistía el escenario de enfrentamiento OTAN – Pacto de Varsovia y los críticos 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 mantenimiento, 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.

Asimismo, la revolución tecnológica y el uso del llamado “bio-terror” ofrecen un futuro cargado de crecientes amenazas y nuevas formas de ataque, mas avanzadas y sofisticadas. Nadie duda que los regímenes adversarios y las organizaciones terroristas tratarán de adquirir y usar armas de destrucción masiva y misiles balísticos para atacar las vulnerabilidades de los Estados Unidos y de otras sociedades abiertas.

Emergencia de nuevos campos de competencia militar. El progreso tecnológico ha dado lugar a la posibilidad de nuevas formas de competencia militar en áreas como el espacio y la cibernética. El espacio y las operaciones de telecomunicaciones e información se han convertido en la columna principal de nuevas capacidades civiles y militares que están transformando el mundo. Se aprecia también que en el dominio del espacio subyace un elemento crucial para la seguridad de USA. Pero, una vez más, toda la arquitectura espacial de USA con sus estaciones, plataformas de lanzamiento y satélites en órbita pueden ser amenazados por capacidades disruptivas que hoy pueden ser accesibles a enemigos potenciales. Esto ha llevado a la convicción de que asegurar el uso del espacio y negar este uso espacial al adversario será un objetivo clave en la competencia militar futura. Al respecto se señala que existen Estados que están desarrollando capacidades de operación ofensivas destinadas a atacar sistemas de información militar y comercial en el mundo.

Creciente potencial de error y del factor sorpresa. Si se observa en conjunto estas tendencias de cambio tecnológico se puede apreciar que hay un creciente potencial de errores de cálculo e información y del uso del elemento sorpresa. Esto se ha apreciado en años recientes en la inesperada velocidad con que algunos Estados han progresado en el desarrollo de armas de destrucción masiva (WMD) así como de misiles balísticos. A futuro se duda que USA sea capaz de predecir con antelación y precisión el progreso de otros Estados en materia tecnológica militar y conceptos operacionales.

Estas dudas se extienden a la predicción de con qué rapidez adversarios potenciales o actuales podrán adquirir armas de destrucción masiva junto con sus sistemas de uso. Finalmente esta duda razonable se extiende a cómo se podrá desarrollar en el futuro la competencia en el espacio cibernético y aéreo.

_____o_____

Como se puede apreciar, en el capítulo Transformación Militar en USA, muchos miran este proceso de cambios de la mayor magnitud conocida a nivel de grandes establecimientos militares como un caso de RM en plena y avanzada evolución. Este orden de magnitud corresponde, como se ha señalado, a la magnitud de las amenazas y riesgos convergentes en el mundo de hoy. Es de esperar que los resultados permitan alcanzar un clima de seguridad mejor que el actual.

III PRE-EMPTION: UNA NUEVA DOCTRINA ESTRATÉGICA DE USA.

La aparición de una nueva doctrina estratégica de USA llamada “pre-emption” fue formulada por el Presidente Bush a través de diversos discursos después del 11 de Septiembre desde su famoso discurso ante el Congreso a comienzos del 2002 sobre el Estado de la Unión en que caracterizó un “eje del mal” que incluía a Irak, Irán y Korea del Norte y advirtió que no permitiría que esos países amenazaran a los Estados Unidos con armas de destrucción masiva. Sin embargo lo que fue un párrafo dentro de un discurso presidencial de amplios y variados temas se articuló más y emergió como una posible doctrina en su discurso en Junio de ese mismo año con motivo de la graduación de Oficiales de la Academia de West Point. Con posterioridad en Septiembre de 2002 se adoptó un documento oficial llamado “Estrategia Nacional de Seguridad de Los Estados Unidos de América”. En su nota de aprobación de este documento el Presidente señala: “defender nuestra Nación contra sus enemigos es el primer y fundamental compromiso del Gobierno Federal. Hoy esa tarea ha cambiado dramáticamente. En el pasado los enemigos necesitaban grandes ejércitos y grandes capacidades industriales para poner en peligro a América. Ahora, obscuras redes de individuos pueden traer gran caos y sufrimiento a nuestras costas con menos lo que cuesta comprar un solo tanque. Los terroristas están organizados para penetrar las sociedades abiertas y usar el poder de modernas tecnologías contra nosotros”.

“Para derrotar esta amenaza debemos usar todo instrumento que poseamos en nuestro arsenal: poder militar, mejores defensas de nuestro territorio, refuerzo de la ley, inteligencia, y esfuerzos vigorosos para suprimir el financiamiento del terrorismo. La guerra contra el terrorismo es de alcance global y es una tarea global de duración incierta. América ayudará a las naciones que necesiten nuestra contribución para combatir el terror”. “Los Estados Unidos y los países que cooperan con nosotros no permitiremos que los terroristas puedan desarrollar nuevas bases de operación. El más grave peligro que enfrenta la Nación es la conjunción del radicalismo y la tecnología. Nuestros enemigos han declarado abiertamente que están buscando armas de destrucción masiva. Los Estados Unidos no permitirán que esto suceda”.

Y en un párrafo que tiene más relación con la nueva **doctrina de pre-emption** el Presidente Bush señala: **“Como un asunto de sentido común y autodefensa América tomará acción contra este tipo de amenazas emergentes antes que estas estén definitivamente formadas”**. A continuación el documento Estrategia de Seguridad Nacional de USA señala: “Aunque nos hemos movido desde la confrontación (nuclear) a la cooperación en nuestra relación con Rusia, han emergido nuevos desafíos mortales provenientes de los “estados viciosos y destructivos” (rogue states) así como de terroristas. Ninguno de estos nuevos riesgos tiene el poder de destrucción que llegó a tener la Unión Soviética. Sin embargo, la naturaleza y motivaciones de estos nuevos adversarios, su determinación de obtener un poder de destrucción disponible sólo por las potencia militares y la creciente

impresión de que ellos usarán armas de destrucción masiva contra nosotros hace que el ambiente de seguridad actual sea mucho más complejo y peligroso a partir de los años 90' hemos presenciado la emergencia de un pequeño número de Estados "viciosos y destructivos" (rogue-states) que, a pesar de sus diferencias, tienen varios atributos comunes. Estos rasgos son :

- brutalizar su propio pueblo y saquear los recursos nacionales para la clase dirigente;
- no respetar la ley internacional, amenazar a sus vecinos y violar los tratados internacionales que han firmado;
- muestran determinación de adquirir armas de destrucción masiva así como otras tecnologías militares avanzadas para usarlas como amenaza o ataque conforme los designios agresivos de estos regímenes;
- patrocinar el terrorismo a nivel mundial;
- rechazar los valores humanos básicos y odiar a los Estados Unidos y todo cuanto este representa.

El documento continúa señalando que durante la Guerra del Golfo, USA tuvo la convicción de que Irak no sólo tenía y había usado armas químicas contra Irán y contra su propio pueblo sino que buscaba adquirir armas nucleares y agentes biológicos (antrax). Más adelante señala que USA debe estar preparado para detener estos estados agresivos y a sus clientes terroristas **antes que alcancen a amenazar o ser capaces de usar armas de destrucción masiva contra USA, sus aliados y amigos.** Este último párrafo

oficial apunta al corazón de la doctrina de pre-emption que está basada en el concepto de atacar un enemigo que represente un peligro inminente neutralizando ese peligro a través de una acción anticipatoria.

El documento Estrategia de Seguridad Nacional de USA describe a continuación los puntos esenciales de la estrategia para combatir el uso de armas de destrucción masiva. En primer lugar, destacan los esfuerzos para una activa contra-proliferación. Aquí se señala que se debe detener y defender la amenaza de las WMD antes que se puedan usar. A este efecto hay que asegurar una capacidad de detección, de defensa activa y pasiva y de contra-ofensiva desarrolladas dentro del proceso de transformación de la Defensa y de los sistemas de seguridad doméstica. Se señala que estos esfuerzos de contra-proliferación deben estar integrados en la doctrina, entrenamiento y equipamiento de las fuerzas de USA y sus aliados de manera de asegurar que superarán cualquier conflicto con adversarios que posean WMD. El segundo aspecto destacado es reforzar las acciones que frenen la proliferación especialmente aquellas destinadas a impedir o prevenir la adquisición materiales, tecnologías y know-how necesarios para armar WMD por parte de los “rogue-state” y terroristas. A este efecto se señala la necesidad de reforzar el control de armas, el control multilateral de exportaciones llegando incluso a interceptar alguna de estas tecnologías y materiales.

El documento que se comenta señala a continuación que a USA le ha tomado varios años comprender la verdadera naturaleza de esta nueva amenaza y que los Estados Unidos no pueden depender solamente de una posición reactiva como ha sido ha ocurrido en el pasado frente a las nuevas amenazas. Así se afirma que frente a la inminencia de ataques en la época actual con la magnitud y potencial de daño que pueden alcanzar las armas del adversario **USA no puede permitir que sus enemigos ataquen primero.**

Elaborando sobre un párrafo de tanto significado como el anterior donde subyace el trasfondo de acción anticipatoria que es como la razón de ser de la doctrina de pre-emption el documento sobre Seguridad nacional señala que en la Guerra Fría, especialmente después de la crisis de los misiles en Cuba, se mantuvo una posición de statu-quo donde el “deterrence” (detención) representó un mecanismo efectivo de defensa. Pero el “deterrence” está basado en el gran riesgo de destrucción y muerte que representa la amenaza de contra-ataque nuclear pero esta consideración puede no tener mucho valor en el caso de líderes terroristas o de “rogue states” que desprecien las vidas humanas o de sus pueblos y estén dispuestos a correr toda clase de riesgos. Se recuerda asimismo que en la Guerra Fría las **armas nucleares, que son de destrucción masiva, eran consideradas como un último recurso** dado que su empleo arriesgaba la destrucción de los que las usaran. Esto no ocurre con el caso con los actuales o potenciales enemigos de hoy quienes **ven a las armas de destrucción masiva como primera opción de uso.** Se sabe que en algunos casos estas armas se han usado como de

intimidación y de agresión militar contra países vecinos como en el caso de la guerra Irak – Irán, de allí que se aprecie que las WMD les pueden permitir a estos estados del “eje del mal” y a los terroristas chantajear a los Estados Unidos y desafiar con su uso hasta la misma superioridad militar de Estados Unidos.

En otros párrafos se señala que durante siglos la ley internacional ha reconocido que las Naciones no necesitan sufrir un ataque antes de que puedan defenderse con todo derecho contra fuerzas que presenten un riesgo inminente de agresión. Como se sabe esta es la norma aceptada por las Naciones Unidas y conocida como **auto-defensa**. En este punto crucial se señala que los expertos juristas a menudo condicionan la legitimidad de una acción de “**pre-emption**” a la existencia de una amenaza inminente referida a menudo como una movilización visible de ejércitos, marinas o fuerzas aéreas preparándose para atacar pero en el tiempo actual se señala que no se prevé que los “rogue states” y terroristas empleen fuerzas convencionales para atacar. Este tipo de ataques estarían condenados al fracaso. En reemplazo ellos descansan en actos de terror y, eventualmente, en el uso de armas de destrucción masiva de un tipo que pueda ser ocultado, depositado en secreto y usado sin ninguna advertencia previa. Todo lo anterior obliga entonces a adaptar el concepto de amenaza inminente vista no sólo como un ataque convencional sino de acuerdo a las capacidades y objetivos de los adversarios de hoy.

Además, se recuerda que, en el caso de este tipo de ataque con WMD, los objetivos serán no sólo las fuerzas e instalaciones militares sino que la población civil violando una de las reglas básicas de las leyes de la guerra.

De todo lo anterior el documento de Seguridad Nacional afirma que Estados Unidos ha mantenido desde tiempo una opción abierta para tomar acciones de “pre-emption” para contrarrestar un riesgo apreciable contra la seguridad nacional del país. A mayor riesgo de amenaza se señala que mayor es el riesgo de la inacción a la vez que es más urgente adoptar acciones anticipatorias para defenderse, aún si la incertidumbre alcanza a no conocer ni el momento ni el lugar del ataque enemigo. Después de esta afirmación terminante de determinación de acciones de “pre-emption” se indica que Estados Unidos no usará la fuerza en todos los casos de amenazas emergentes y se pide a otros países que no se use las acciones de “pre-emption” como un pretexto para una agresión (i). La verdad que este último párrafo en que se trata de atenuar la inmensa peligrosidad de esta doctrina de guerra resulta imposible de no calificarlo como un rasgo autoritario extremo al darse el derecho a atacar y negarlo a otros países que puedan vivir situaciones similares.

Por fortuna el documento oficial en este capítulo se completa con algunas consideraciones que atenúan algunos de los terribles alcances de la doctrina de “pre-emption”. Así se señala al respecto que “USA procederá en cada caso con una cuidadosa deliberación previa sopesando todas las consecuencias de sus acciones”. Además se declara que se desarrollaran

capacidades de inteligencia integradas y precisas de manera que se cuente con una información comprobada y oportuna sobre las amenazas donde quiera que estas emerjan. En el mismo sentido USA se compromete a trabajar mas coordinadamente con sus aliados para llegar a una apreciación común de las amenazas más peligrosas. Y en un anticipo de los que es la gran variación de la estrategia militar se declara que USA **continuará transformando su fuerza militar para asegurar su capacidad de conducción de operaciones bélicas rápidas y precisas que permitan alcanzar resultados decisivos.**

El párrafo final de este capítulo señala: “el propósito de nuestras acciones será siempre eliminar una amenaza específica a los Estados Unidos o a sus aliados o amigos. La razón de nuestras acciones será clara, la fuerza medida y la causa justa”.

Recopilación de Comentarios sobre la doctrina de pre-emption.

El primer comentario proviene de una voz tan autorizada como el del entonces Secretario de Estado Colin Powell que escribía en Foreign Affairs de Febrero de 2004 sobre el unilateralismo y las guerras de tipo “pre-emptive”: “la Estrategia Nacional de Seguridad explicitó el concepto de “pre-emption” después de septiembre 11 y lo hizo por razones obvias. Una primera razón fue asegurar al pueblo americano que poseemos sentido común.. Como ha dicho el Presidente Bush, y cualquier persona sensible lo comprende, si Ud. identifica una amenaza nítida y presente que es indetenible (undeterrable) por los medios que se dispone, entonces hay que enfrentarla. Ud. no espera ser atacado; Ud. no permite que ocurran nuevos ataques sin tomar acción”.

Con este comentario el ex - Secretario Powell justifica la acción de “pre-emption” ante una amenaza “nítida y presente” añadiendo un rasgo adicional de tratarse una amenaza **donde no es posible aplicar el “deterrence”**. Hay que recordar que el concepto de deterrence proviene de la época de Guerra Fría y habitualmente implica el uso de la amenaza nuclear y que se entiende casi siempre como una respuesta masiva mas bien a Estados que a grupos terroristas. En todo caso el Secretario Powell mantiene el rasgo de acción **militar anticipatoria** que tiene el concepto estratégico de pre-emption. Sin embargo el Secretario de Estado dejó abierta la puerta a la opción de

“deterrence” como una justificación del “pre-emption”. Así señala: “Una segunda razón para incluir la noción de “pre-emption” en la Estrategia Nacional de Seguridad fue comunicar a nuestros adversarios que estaban ante un gran problema. Al instilar una cierta cantidad de angustia en grupos terroristas aumenta la posibilidad de que ellos cesen su actividad o cometan errores y sean capturados. Más aún, se da una advertencia a algunos Estados que han sido cómplices con terroristas no por razones ideológicas sino oportunistas. En este sentido vale la pena notificar a los líderes de esos países del gran riesgo de pagar altos costos por su oportunismo”.

Más adelante el Secretario Powell continúa sus explicaciones diciendo:

“a pesar de estos razonamientos, algunos observadores han exagerado tanto el ámbito del “pre-emption” en la política exterior como en la centralidad de este concepto en la estrategia de USA. En el ámbito del pre-emption **éste se aplica sólo a amenazas no controlables por el deterrence tales como las que provienen de actores no - estados como son los grupos terroristas**”. Y añade: “Nunca se intentó desplazar el deterrence (por pre-emption) sino que suplementarlo. En cuanto a un rol central del pre-emption, **este no existe**. La discusión de pre-emption en la estrategia nacional de seguridad ocupa sólo una mínima parte de un documento oficial de ocho secciones”.

En estos comentarios se advierte la búsqueda de una opción abierta de **mantener el deterrence junto con el pre-emption** visualizando ventajas frente a cada caso de amenaza provenga esta de un estado o de un grupo no estado como es el caso del terrorismo. Sin embargo no se entra en precisiones de lo que constituye una amenaza “undeterrable”. Al respecto se puede asumir que esto ocurre en el caso de ataques terroristas suicidas ante los cuales no se puede esperar una reacción masiva contra un grupo pequeño. Pero, en todo caso, parece apoyarse la acción de pre-emption como dotada de un efecto de deterrence.

Mirando en retrospectiva este documento de 2004 de una personalidad de tanta experiencia se registra una discordancia en sus propósitos por cuanto los ataques terroristas de Madrid y de Londres revelan el peligro potencial y permanente de nuevos ataques ante los cuales ni el “deterrence” ni el “pre-emption” tienen aplicación.

Otros comentarios vienen de un documento de investigadores de la Brookings Institution del año 2004 en que se hace una evaluación del concepto de “pre-emption” señalando que la Administración Bush argumenta que la pre-emption debe extenderse e incluir “ataques preventivos” aún en la ausencia de una amenaza inminente. A este respecto es importante recordar que el concepto de **acción militar preventiva** (prevention) está mucho menos aceptado en la ley internacional aunque Estados Unidos lo ha utilizado y amenazado en otras épocas. Esto se analiza más adelante. Tal fue el caso, por ejemplo, en 1994 cuando Estados Unidos señaló públicamente que no permitiría que Korea del Norte

desarrollara su arsenal nuclear. Esta fue una clara amenaza de acción preventiva cuya discusión continúa hasta nuestros días. Otros ejemplos de acciones **preventivas** de Estados Unidos son la invasión de Grenada en 1983 y el intento de la invasión de Cuba en la bahía de Cochinos en 1961. De ahí que hoy en día la aplicación de acciones preventivas sobre grupos terroristas bien identificados no despierte mayor controversia. El problema radica en que estos actores actúan con gran secreto y ocultamiento para aprovechar el factor sorpresa de sus ataques de allí que resulta casi imposible identificar anticipadamente donde y como atacarán en el futuro.

De este modo el requisito de una amenaza inminente disminuye y se debe recurrir a opciones más tradicionales como las acciones preventivas. Pero el problema es diferente cuando se trata de la amenaza de los llamados “rogue states”. En este caso, el panorama se complica aún más al ser difícil distinguir entre la eliminación de capacidades peligrosas y derrocar regímenes adversarios. En este último caso se entra en un campo de amplias consecuencias para la estabilidad del sistema internacional y se entrecruza esta acción con el riesgo de uso de armas de destrucción masiva (WMD) que esta estrategia pretende controlar. Sin embargo tomar acción para neutralizar capacidades ofensivas tiene resultados mas limitados, como fue el caso del ataque de la administración Clinton en 1998 contra las supuestas instalaciones de WMD en Irak, luego que Hussein prohibiera las inspecciones de la UN. Al final, las opciones políticas no pueden descartar el derrocamiento de regímenes en casos extremos pero esto debería considerarse sólo como una última opción ante la imposibilidad de eliminar capacidades peligrosas por otros medios.

En otro comentario de estos investigadores se señala que hay otras dos preocupaciones importantes alrededor de la doctrina de pre-emption como estrategia oficial de USA. Primero, que la pre-emption devalúa el aún importante rol de la deterrence incluida las acciones contra los “rogue status” como Irak y Korea del Norte. Segundo, que el pre-emption legitima el uso de la fuerza en un ámbito mayor cual es que ésta se puede emplear **sin una amenaza clara, inminente y ampliamente aceptada**, posición que se opina que Estados Unidos no debiera apoyar.

Otro ámbito de consideraciones de este trabajo es sobre los peligros de legitimar las acciones de pre-emption. Esta es una de las mayores preocupaciones en todos los ámbitos respecto de cual es el impacto y alcance del precedente sentado por Estados Unidos legitimando estas acciones lo que puede llevar a otros a emular esta conducta reduciendo así la ventaja para convencer a otros países que no deban usar la fuerza. Al respecto se señala que esta preocupación es teórica en cierto nivel pero en otro sentido es muy real y aunque hoy día las guerras entre estados son relativamente infrecuentes el entregar fundamento a otros países para tomar acciones de pre-emption ante un umbral de amenaza menor puede jugar en contra de esta doctrina y exacerbar crisis regionales que a veces están al borde de un conflicto abierto. En otras palabras que corresponden a un comentario del CEES, no se aprecian razones para que sólo Estados Unidos pueda adoptar medidas de pre-emption y nó otros regímenes o estados soberanos aduciendo el peligro de una amenaza inminente que justifique desatar un conflicto. En este caso la gran pregunta e incógnita sería la

conducta de USA si llegara a condenar a un estado soberano por hacer algo análogo al amparo de una doctrina de pre-emption como la legitimada por ese país. Los ejemplos potenciales de esta última posibilidad no son pocos y van desde los casos de Etiopía e Eritrea, China y Taiwan hasta el Medio Oriente. Sin embargo el caso más claro es la situación existente entre India y Pakistán, dos países poseedores de armas nucleares. En este último caso la política de pre-emption legitimada por USA entrega más argumentos a los halcones en India para justificar un ataque contra Pakistán. Un último caso en este riesgoso panorama es el caso de Rusia y sus amenazas recientes contra el estado de Georgia y la guerra contra extremistas islámicos en Chechenia.

Como se aprecia, legitimar una doctrina de pre-emption conlleva numerosos peligros y de allí el gran debate internacional respecto de este concepto. De allí que la política exterior de Estados Unidos haya ido ajustándose ante un panorama internacional complejo. Así, en 2002 la hoy día Secretaria de Estado Condoleezza Rice enfatizó en un discurso en el Instituto Manhattan que el pre-emption debe ser usado sólo después que se han agotado otras soluciones y, de manera principal, en casos en que surja una grave amenaza. Asimismo añadió que “los riesgos de esperar deben sobrepasar con mucho a los riesgos de la acción”

El Debate Internacional acerca de la Auto-Defensa.

Completamos este estudio sobre la doctrina de pre-emption preconizada por la Administración Bush con un comentario internacional proveniente de la esfera de analistas de estos temas en el ámbito de Naciones Unidas.

El debate legal acerca del significado del concepto de “auto-defensa” en las cambiantes condiciones de la era actual está centrado en el significado exacto que está incluido en las palabras claves del Artículo 51 de la Carta de Naciones Unidas: Este artículo dice “nada de esta Carta impedirá el derecho inherente a la auto-defensa individual o colectiva en el caso de que ocurra un **ataque armado** contra un Miembro de Naciones Unidas”. Este es el único artículo de la Carta que acepta el uso de la fuerza por estados miembros actuando independientemente. Como se ha dicho, el debate se centra en la interpretación que se dé a la expresión **ataque armado**. En la interpretación de este artículo, la mayoría de los internacionalistas concuerda que este artículo simplemente recoge y reconoce un antiguo derecho a la auto-defensa por parte de la Carta. Sin embargo la interpretación no es tan unánime cuando se plantean dos preguntas fundamentales. La primera es ¿se puede considerar como un **ataque armado** una acción que proviene de cuerpos ó grupos sin-estado como es el caso de grupos terroristas? En segundo lugar: ¿debe existir un ataque armado real y actual antes de ejercer el derecho de auto-defensa y puede un estado actuar para controlar un ataque inminente?

En la práctica, la interpretación del Art.51 de la noción de “ataque armado” es bastante difícil. El Art. 51 no especifica si un ataque armado tiene que provenir de un estado ni si este debe ser de una forma convencional. Con todo, hay un fuerte reconocimiento de que un ataque terrorista mayor o una campaña terrorista sostenida puede constituir un “ataque armado”. Al respecto el Consejo de Seguridad de la UN reconoció en su resolución 1368 del 12 de Septiembre de 2001 “el derecho inherente de la auto defensa individual o colectiva de acuerdo con la Carta”. Esto ocurrió al día siguiente del ataque terrorista contra USA y fue una luz verde del Consejo para la actuación militar de Estados Unidos en Afganistán. Esta Resolución apoyó el principio de la auto- defensa ante un ataque terrorista, sin embargo en este caso había una evidencia importante de que un estado como Afganistán amparaba las actividades que desembocaron en estos ataques. De este modo quedó abierta la cuestión de qué tipo de respuesta sería permitida en caso de ataques terroristas por grupos sin-estado o en casos que la acción de estos grupos no tiene claro respaldo de un estado.

De este modo, el debate sobre “pre-emption” y “prevention” continúa con un incremento aparente de la aceptación a las acciones pre-emptivas. Sin embargo, la **acción militar preventiva** entendida como aquella que tiende a anular una **amenaza futura** y no inminente resulta mas problemática. Como se sabe este concepto está incorporado en la Estrategia Nacional de Seguridad de USA. Sin embargo esta llamada “acción preventiva” no tiene mucho eco y respaldo internacional por las mismas razones que los cuerpos internacionales han sido renuentes a enunciar o apoyar un derecho general

de los estados para intervenir militarmente aún en el caso de las llamadas “razones humanitarias”. En este último caso, a pesar de la fuerza y del impacto de la razón humanitaria se ha preferido limitar el apoyo a la acción militar sólo a casos de auto-defensa urgente e inmediata sin extenderlo más allá por temor a un uso abusivo de intervenciones militares.

En todo caso hasta ahora la ley internacional no autoriza un ataque militar de un estado ante una amenaza de largo plazo o remota, de allí que la acción preventiva, si nó cuenta con la aprobación del Consejo de Seguridad, puede intentar entrar en el dominio de la auto-defensa. Por ejemplo, ¿que ocurre si es evidente que existe un grupo terrorista en un territorio definido está equipado con armas nucleares pero no existe claridad en contra de quien podrían usarse estas armas? En este caso existiría una amenaza real a la paz y seguridad internacional y el Consejo de Seguridad de UN tendría título para actuar. Sin embargo si el Consejo de Seguridad no actúa sea por votación negativa o veto y un estado quisiera actuar sería artificial justificar su acción como auto-defensa, pero esta eventualidad existe.

En esta discusión se cuenta con la opinión autorizada de dos cuerpos internacionales como son la Corte Internacional de Justicia y el llamado Panel de Alto Nivel de la NU. Ambos cuerpos han sido críticos para reconocer un derecho no calificado de los estados para adoptar acciones militares de intervención como respuesta al terrorismo. Las observaciones del Tribunal Internacional de Justicia relativas al art. 51 en particular se han prestado a controversia como en el fallo reciente sobre las consecuencias legales de la construcción del muro por Israel en los territorios palestinos

ocupados. En este caso, el Tribunal dio una interpretación restringida del concepto de ataque armado cuando proviene exclusivamente de estados. Esto ha dado fuerza a la opinión de muchos juristas en el sentido que los actos de terrorismo cometidos por grupos o organización privados no caen en el significado de “ataque armado” del art. 51. Sin embargo estas opiniones podrían significar que los estados no tienen derecho a auto-defensa contra ataques piratas, de bárbaros o de bandas armadas a menos que tuviesen una conexión con un estado en particular. Esto choca sin duda con el reconocimiento histórico del derecho de los estados a defenderse ante ataques de este tipo.

Por su parte el informe del Panel de Alto Nivel de la UN sobre Amenazas, Desafíos y Cambios se dio a conocer a fines del 2004 bajo el título “Un Mundo Más Seguro”. Una de sus tareas centrales fue analizar las circunstancias en las que la seguridad colectiva puede requerir el respaldo de la fuerza militar comenzando con las reglas de la ley internacional que deben gobernar cualquier decisión de ir a la guerra para que la anarquía no prevalezca. Así el informe señala: “hay poca evidencia de una aceptación internacional a la idea de que la seguridad se preserva mejor por un balance de poder o por una sola superpotencia por muy bien intencionada que esta sea”. Mas adelante, al discutir el significado de la auto-defensa bajo el art. 51 de la Carta el informe analiza la legalidad de las acciones militares tipo “pre-emption” y tipo “preventive”. Al respecto dice: “un Estado amenazado, de acuerdo con la ley internacional establecida mucho tiempo,

puede adoptar acción militar en caso de que la amenaza de ataque sea inminente, si no existen otros medios para frenarla y si la acción es proporcional. El problema se suscita cuando la amenaza en cuestión no es inminente pero se la señala como real como en el caso de la adquisición de una capacidad de fabricación de artefactos nucleares con una intención que se atribuye como hostil”.

“Puede un Estado no recurrir al Consejo de Seguridad y reclamar su derecho a la acción como un acto de auto-defensa anticipatoria no solo a través de una acción contra una amenaza inminente (pre-emption) sino contra una amenaza no inminente y no cercana (preventive)? Aquellos que responden afirmativamente argumentan que el daño potencial de algunas amenazas como el caso de armas nucleares en manos terroristas es tan grande que nadie puede correr el riesgo de esperar hasta que la amenaza se haga inminente y que se puede actuar cuando se corre menos riesgo anticipando que esperando”.

La respuesta del Panel es que si hay buenos argumentos para una acción militar preventiva con buena evidencia que la apoye estos casos deberían ponerse en manos del Consejo de Seguridad el que puede autorizar tales acciones si así lo decide. Si no se concurre al Consejo debiera usarse el tiempo en estrategias de persuasión, negociación, contención y deterrence al tiempo que se revisa la acción militar. Para aquellos impacientes por tener una respuesta a la cuestión planteada esta debe ser que, en un mundo lleno

de amenazas potenciales, el riesgo de alterar el orden global y la norma de no intervención, que siguen siendo básicos es simplemente demasiado grande para reconocer la legalidad de una acción preventiva unilateral. Permitir esta acción en un caso es permitirlos en todos”.

Como conclusión el Panel señala “no favorecemos re-escribir ni re-interpretar el art. 51 de la Carta”. Otras conclusiones del informe recalcaron la verdad aceptada de que el Consejo de Seguridad de UN es un cuerpo dotado de toda la autoridad para autorizar acciones militares del tipo pre-emption o preventive a la vez se reafirma la autoridad del Consejo de Seguridad para ejercer la llamada “responsabilidad de proteger” en los casos que autoriza intervención militar para detener matanzas de gran escala entre Estados. Sin embargo, aún el propio Consejo de Seguridad debe tener en cuenta consideraciones sobre la legitimidad de sus resoluciones. En este sentido el Panel formuló algunos **criterios básicos de legitimidad** que debieran estar presentes cuando el Consejo endosa el uso de la fuerza. Se trata de cinco criterios de legitimidad:

- Gravedad de la amenaza
- Propósito adecuado
- Ultimo recurso
- Proporcionalidad de medios
- Equilibrio de resultados

Como se aprecia, estos cinco criterios son útiles, pero no todos pueden cumplirse acumulativamente sin problemas.

A pesar de este avance en el terreno de legitimar el uso de la fuerza aun falta saber que ocurre en los casos que el Consejo de Seguridad no logra acuerdo ante una situación de auto-defensa o de responsabilidad de protección. De allí que se opine que estos criterios de legitimidad están más dirigidos a los estados mismos o a las coaliciones que se forman frente a ciertas amenazas. Como persiste el caso de Estados que usen la fuerza sin recurrir al Consejo de Seguridad el Panel cree que Naciones Unidas debe tratar de establecer un “sistema de seguridad colectiva”. A este respecto el Panel hace referencia a un sistema de seguridad internacional centrado en UN que pueda manejar una amplia gama de amenazas. Sin embargo se sabe que estos intentos han existido en el pasado pero han enfrentado grandes dificultades de aprobación en un foro político como es Naciones Unidas.

El informe del Panel goza de respeto por parte de los gobiernos. Ya aportó en la difícil tarea de definir el terrorismo y ha manifestado su preocupación ante una amplia gama de amenazas así como en asuntos de cooperación en seguridad. Por eso su sugerencia que el art. 51 de la Carta no debiera ser re - escrito ni re - interpretado parece un sabio consejo. Sin embargo el informe contribuye notablemente a una interpretación del art. 51 favorable al reconocimiento legal del principio de acciones de pre-emption contra ataques inminentes bajo ciertas circunstancias.

Proposiciones de Salvaguardas ante una Concepción Amplia de Auto-Defensa.

Como se ha visto el concepto de auto-defensa tiene defensores que buscan ampliar su aceptación y legitimidad. Sin embargo no hay un acuerdo general para una nueva fórmula de redacción sobre este tema. A pesar de esto, un Comité Asesor de la Corte Internacional de Justicia ha sostenido que hay una abundante cantidad de opinión en el sentido que el derecho a la auto defensa alcanza y comprende dos principios: uno, el derecho de los Estados a realizar acciones de pre-emption con el propósito de eliminar el peligro de un ataque inminente desarmando a un enemigo amenazador. Segundo, el derecho de los Estados a adoptar acciones en respuesta al terrorismo internacional. La aceptación de estos dos principios por un Tribunal internacional significa un reconocimiento parcial a las realidades y lecciones de la historia de que los Estados y sus ciudadanos son proclives a la idea de tomar acción para reducir o eliminar ataques que se perciben como inevitables o a la vez que son renuentes a esperar que estos ataques ocurran para responder. Asimismo, se considera aceptable adoptar respuestas militares apropiadas ante el riesgo terrorista. Sin embargo se sigue advirtiendo de los riesgos que existen de abrir la puerta a acciones militares de los Estados. En este último caso se señala que los riesgos pueden ser realmente serios en el caso de las acciones de “pre-emption”. Por ejemplo, se señala que el concepto de “inminencia” de un ataque debe indicar una intención, capacidad, planes y preparativos para atacar pero es difícil producir la evidencia necesaria de todas estas actividades a tiempo y antes

de tomar la decisión de acción anticipatoria. En verdad se señala que la pre-emption puede depender más en juicios subjetivos que en evidencia respecto de un ataque inminente. Incluso la información de inteligencia puede ser incompleta y sesgada. Todo esto se vio reflejado en el caso de la guerra en Irak donde el Presidente Bush acaba de reconocer que hubo errores en la inteligencia analizada. También se da el caso de Estados que pueden ser escépticos de las acciones de pre-emption que adopten otros Estados. Para evitar el riesgo de abusos en el derecho a una acción de pre-emption se debería exigir un alto estándar de pruebas de la amenaza y estas pruebas deberían ser verificadas por procedimientos adecuados al nivel de los gobiernos. Como se ha dicho, estas consideraciones son más claras en el papel que en la realidad al comprobarse que las fallas en la apreciación y el proceso de toma de decisiones en el caso de Irak levantó una gran sombra sobre la doctrina de pre-emption de la administración Bush.

El récord histórico de guerras contra fuentes o grupos terroristas no es muy grande. Los casos de acción militar contra ataques terroristas en Serbia en 1914, Líbano en 1982 e Irak en 2003 no sostienen ni despiertan simpatía para dar una autorización internacional amplia a la acción militar.

Por último todas estas consideraciones del ámbito internacional parecen apuntar a una conclusión simple: aun si se acepta que ciertos tipo de ataque terrorista pueden ser catalogados como “ataque armado”, esto no puede considerarse como un permiso automático para responder militarmente sin tomar en consideración y con la debida prudencia toda clase de factores.

Más aún y precisamente porque se trata de un asunto debatible el uso de la fuerza militar parecería tener mas legitimidad en caso de una respuesta multilateral que en una respuesta unilateral

En suma, el debate internacional sobre la legitimidad de las acciones de “pre-emption” y “prevention” a nivel militar no tiene aún una aceptación definitiva y es muy probable que las interrogantes que despierta continúen presentes.