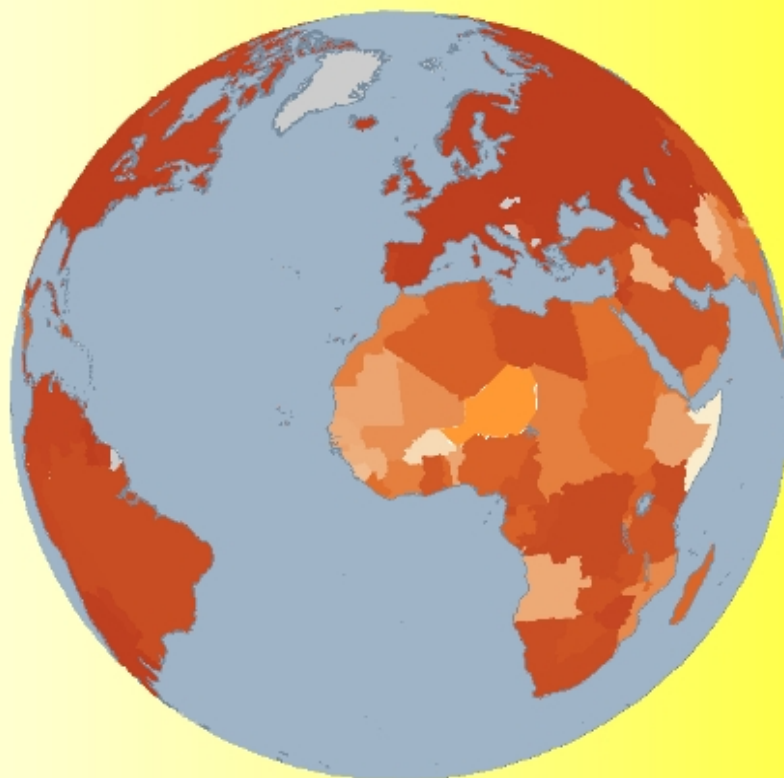




DOCUMENTOS

DE SEGURIDAD Y DEFENSA



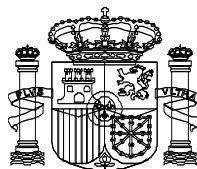
ADAPTACIÓN
DE LA FUERZA CONJUNTA
A LA GUERRA ASIMÉTRICA



CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

***ADAPTACIÓN
DE LA FUERZA CONJUNTA
A LA GUERRA ASIMÉTRICA***

Septiembre de 2011



MINISTERIO DE DEFENSA

ÍNDICE

	<u>Página</u>
INTRODUCCIÓN.....	7
<i>Por José María Terán Elices</i>	
AMENAZAS: CAMBIO, ADAPTACIÓN E INNOVACIÓN MILITAR.....	00
<i>Por Enrique Fojón Lagoa</i>	
LA EVOLUCIÓN DEL PARADIGMA ESTRATÉGICO OCCIDENTAL EN EL MUNDO GLOBALIZADO.....	00
<i>Por Guillem Colom Piella</i>	
CIBERESPACIO: LA NUEVA DIMENSIÓN DEL ENTORNO OPERA- TIVO.....	00
<i>Por Ángel Sanz Villalba y Enrique Fojón Chamorro</i>	
CONCLUSIONES.....	00
<i>Por José María Terán Elices</i>	
COMPOSICIÓN DEL GRUPO DE TRABAJO.....	00

INTRODUCCIÓN

Es España un país en el que las cuestiones relacionadas con la seguridad y defensa son tradicionalmente poco consideradas por gran parte de la población. Un país en el que existen muy pocos grupos de pensamiento dedicados a estas cuestiones, que además, en general, suelen estar muy condicionados y en el que, por consiguiente, no se crea no ya una corriente de opinión pública, sino que las propias élites dirigentes no asumen plenamente la conciencia de esta realidad. En estas circunstancias, es difícil que un título como el que define el presente Documento de Seguridad y Defensa: «La adaptación de la fuerza conjunta a la guerra asimétrica» pueda tener una aproximación homogénea en la percepción del alcance que pueda tener su contenido.

Tampoco creo que en el ámbito profesional militar español, fuera de los órganos especializados, haya un pensamiento arraigado sobre la cuestión, un cierto corporativismo por parte de algunos, todavía hoy latente en el sustrato más profundo de los Ejércitos y la Armada, o la falta de visión de futuro de otros, han impedido o cuando menos dificultado, la consolidación de un modelo de pensamiento militar. Ese anquilosamiento que hemos sufrido durante algunos años tenía forzosamente que reflejarse en el pensamiento estratégico nacional.

Es posible que, aún hoy, en el ámbito militar no esté totalmente asumido el concepto de fuerza conjunta al que se refiere este Documento. «En lo más profundo de algunos corazones» está todavía conceptualmente arraigada la existencia de las operaciones específicas independientes como elemento marcadamente diferenciador entre los Ejércitos y la Armada. Esta realidad ha influido notablemente en el desarrollo de la concepción de la estrategia militar española, muy condicionada por el pensamiento táctico y, sobre todo, por la tradicional diferente visión estratégica que ha existido entre los tres componentes militares.

La Defensa Nacional y con ella la organización militar, estuvo regulada en España durante 25 años por una ley surgida en la Transición cuando todavía los ajustes de poder

eran complejos y hasta frágiles y cuyos planteamientos, estaban más próximos a los vigentes antes de la Segunda Guerra Mundial que a los que ya imperaban en el mundo occidental al comienzo de la década de los años ochenta. En esos años hubo intentos lúcidos de modificar la situación pero un conservadurismo exagerado los obstaculizó sistemáticamente.

El poder político, al que definitivamente estaban sometidas las Fuerzas Armadas, tampoco ayudó mucho a modificar esta situación posiblemente por sentirse cómodo en ella, ya que mantenía razonablemente satisfechos a los mandos militares a cambio de repartir, en la mayor parte de las ocasiones proporcionalmente, los escasos presupuestos del Ministerio de Defensa.

La aprobación de la nueva Ley de la Defensa Nacional en el año 2005 ha permitido, después de más de 20 años, dar un paso decisivo para abordar las reformas que ya resultaban imprescindibles con el fin de no perder el tren de la nueva concepción de la estrategia, de las operaciones e incluso de la táctica, reformas que habían venido fraguándose, desde algún tiempo atrás, con la implantación de la plena profesionalización y, sobre todo, con la elaboración y promulgación de la Revisión Estratégica de la Defensa del año 2003 consensuada, en buena medida, entre los dos grandes partidos con posibilidad de diseñar y desarrollar la estrategia.

La promulgación de la nueva Ley de Defensa Nacional, aunque es cierto que podía haber ido más allá en su concepción, ha permitido reconducir, en buena medida, la situación y progresar hacia esa adaptación al planteamiento de la Defensa, ya generalizado entre nuestros aliados.

Sin embargo, esa adaptación que se ha producido en buena forma en el mundo militar, no se ha visto reflejado en la sociedad en su conjunto, posiblemente por el uso eufemístico del concepto de ayuda humanitaria para justificar el empleo de las Fuerzas Armadas en escenarios de evidente enfrentamiento armado que, sin duda, y en cierta forma paradójicamente, han acrecentado el prestigio de éstas, pero que no ha ayudado a la concienciación social sobre los cambios que en estos años se han producido en la naturaleza de las amenazas, la estrategia y las operaciones y lo que es peor aún, en el papel que un país como el nuestro debe jugar en el concierto de las relaciones internacionales.

Estas circunstancias tienen lugar en un escenario mundial que no ha ayudado a que las dificultades señaladas en el ámbito interno pudieran ser superadas con mayor facilidad. Los cambios han sido tan importantes y rápidos, que las propias organizaciones

internacionales relacionadas con la seguridad y defensa a las que pertenece España, no han estado muy prestas a la hora de liderar ese mundo.

Tras la caída del muro de Berlín, la Organización del Tratado del Atlántico Norte (OTAN) ha perdido, en buena medida, el protagonismo que durante el período de la guerra fría desempeñó y poco a poco ha ido distanciándose del liderazgo que sobre la estrategia de seguridad mantuvo a lo largo de muchos años. El notable incremento del número de miembros que, sin la menor duda, ha ayudado a estabilizar la Europa Oriental tras la desaparición del Pacto de Varsovia, ha dificultado la consolidación de una línea estratégica avanzada, aunque la razón para esto hay que buscarla en el distanciamiento conceptual de Estados Unidos respecto al resto de los aliados de la OTAN, entre otras causas por su cambio del centro estratégico global hacia el Pacífico.

Después del 11 de septiembre de 2001, las cosas ya no han sido lo mismo que lo fueron hasta entonces, el pensamiento militar norteamericano ha volado sin que la mayor parte de miembros de la OTAN hayan podido o, seguramente querido, seguirlo o modificarlo. Los intereses de unos y otros se han ido distanciando sin que los diferentes conflictos surgidos hayan permitido volver a sintonizarlos completamente.

El Concepto Estratégico de 1999 se hizo añicos tras los atentados de las Torres Gemelas y rehacerlo ha costado varios años, sin que los resultados reflejen la existencia de una organización que pueda afrontar con la misma solvencia que lo hiciera en otra época, las múltiples dificultades que este mundo globalizado nos depara y, lo que puede ser más grave, con toda seguridad nos deparará en el futuro. La fórmula utilizada en la última intervención militar en el norte de África lamentablemente parece reflejar esta realidad.

La Unión Europea, incluso en sus distintas formas pasadas, ha sido siempre un referente conceptual para España, a pesar de que en el ámbito que nos ocupa, nunca ha llegado a tener protagonismo propio. El Documento Solana significó un paso adelante muy notable por lo que representaba para la Política Europea de Seguridad y Defensa (PESD), pero la realidad es que tras algunos escauceos que podían hacer pensar que se estaba en el camino adecuado, ha acabado por quedarse en casi nada.

Tras las dificultades para la aprobación de la Constitución europea que mostraron los serios obstáculos en la consecución de una unidad política, el reciente Tratado de Lisboa marca el nuevo camino para la creación de una Política Común de Seguridad y Defensa (PCSD) mediante la concepción de la Cooperación Estructurada Permanente que,

probablemente como consecuencia de la profunda crisis económica que nos ha tocado vivir, no ha llegado, ni tan siquiera, a definirse conceptualmente.

De momento se puede pensar que, aparentemente al menos, no tenemos PESH europea sin embargo, el nuevo acuerdo firmado por franceses y británicos, que según todo indica tiene un mayor espíritu de permanencia que los anteriores, podría ser embrión de algo. De hecho han sido invitados, en alguna medida, a participar: alemanes, holandeses, italianos y españoles.

En este mundo lleno de dificultades para la evolución en este área, ¿cómo ha podido producirse esta adaptación de la fuerza conjunta, entendida como tal la fuerza utilizada en operaciones, a la guerra asimétrica denominación referida a las guerras que han ido produciéndose en los últimos años y en las que han participado fuerzas de coaliciones más o menos numerosas o de la OTAN, pero todas ellas bajo el liderazgo de Estados Unidos?

Esta es la cuestión que trataremos de aclararles a continuación, o al menos acercarnos a ello, para lo cual nos fijaremos en tres aspectos definitorios: la amenaza, la estrategia y las operaciones.

La cuestión de la amenaza la abordaremos desde un punto de vista conceptual, se analizarán: el cambio producido, la adaptación a ese cambio y cómo no, la innovación que arrastra el cambio.

En el ámbito de la estrategia se analizarán las concepciones estratégicas y las políticas de seguridad desde el final de la guerra fría hasta nuestros días.

El concepto de las operaciones como tal, requeriría, cuando menos, un trabajo como éste para él sólo, por eso me ha parecido más interesante fijarnos exclusivamente en un aspecto de la posible asimetría de la confrontación actual como es la ciberguerra, todavía hoy casi en pañales, al menos en España, pero que se nos viene encima a marchas forzadas, por lo que me parece que cualquier atención que le prestemos será poca.

Estoy convencido que la lectura y el análisis de las aportaciones que vienen a continuación, les permitirán aproximarse al cómo y el porqué se ha producido la adaptación que nos sugiere el título del presente Documento.

JOSÉ MARÍA TERÁN ELICES
Almirante (R)

AMENAZAS: CAMBIO, ADAPTACIÓN E INNOVACIÓN MILITAR

Tratar de cambio en cualquier orden de la vida es tarea ingente, cuando se trata de la institución militar, aparte de colosal, es de la mayor complejidad. Cualquier proceso de adaptación necesita una serie de referencias y en el caso que nos ocupa, el militar, es la Historia a donde parece conveniente mirar. Si los hechos históricos son acontecimientos conocidos y su contexto es objeto de polémica, la interpretación del presente se antoja tarea ardua, por lo tanto, al tratar el tema en cuestión hay que asumir que se corre un riesgo, en este caso intelectual. La existencia de ese tipo de riesgo es un hecho, pues es la base del error.

Podría establecerse que para la última década del siglo XX y la primera del XXI, las fechas más relevantes sean: la caída del muro de Berlín el 9 de noviembre de 1989, los ataques a Estados Unidos el 11 de septiembre de 2001 y la quiebra del banco de inversión Lehman Brothers el 15 de septiembre de 2008. Esas fechas también podrían utilizarse para categorizar el empleo que se hizo de la fuerza militar entre los periodos por ellas delimitados. En ese caso, la caída del muro marcaría el fin de la guerra fría, con ella el de la amenaza de la temida destrucción mutua y el auge de la «guerras de elección», en su modalidad popular de «operaciones de paz». El 11 de septiembre marca el inicio de la «guerra larga», inicialmente denominada Guerra Global contra el Terror (GWOT), con la eclosión del mantra de la Contrainsurgencia (COIN). En cuanto a la quiebra de Lehman Brothers todo parece apuntar a que abrirá una época de «frugalidad» económica, según denominación de Michael Mandelbaum¹, lo que hará más selectivo el empleo de la fuerza.

Este esquema sirve para intentar enmarcar la evolución de la situación estratégica en esos años, deducir sus consecuencias y preparar el camino para afrontar el porvenir. La conciencia de vivir en un ambiente de gran complejidad con un alto ritmo de cambio es el punto de partida de cualquier análisis que intente diseñar las capacidades de la fuerza

¹ MANDELBAUM, Michael: *The frugal superpower*, Public Affairs, Nueva York, 2010.

conjunta en relación con las amenazas presentes y futuras en una situación de conflicto permanente. Esta situación nos lleva a considerar un itinerario que partiendo de la conciencia de cambio, permita adoptar una actitud de adecuación al ambiente cambiante para estructurar la necesaria tarea de innovación.

Cambio

A lo largo de estas dos últimas décadas, académicos, militares y analistas en general, se han afanado en descubrir los genes de una nueva era militar para, de esta manera, intentar establecer y sintetizar aquellos principios inéditos que regirían en época futura. Un peligro que acecha tanto a militares como a los integrantes de los otros dos estamentos nombrados anteriormente, es que, para resolver los problemas del presente y del futuro, orienten sus esfuerzos de investigación hacia la búsqueda de nuevos aspectos de la naturaleza de la guerra en vez de intentar hacer frente a los problemas de su conducción en los ambientes presentes. El profesor Colin S. Gray, recientemente nos pone en alerta sobre este aspecto al señalar que:

«El principal problema al que se enfrentan aquellos a cargo de la función estratégica de la conducción del planeamiento estratégico, para la seguridad nacional, es la necesidad de prepararse prudentemente para un futuro del que casi todo se conoce pero casi nada con el detalle necesario»².

En lo concerniente a la guerra, el cambio, en la continuidad de su naturaleza, está en la innovación de los medios y modos de actuación, con la habilitación del consiguiente marco doctrinal. En la actualidad, el reto se concreta en la adaptación a un ambiente fluido, en permanente cambio, tanto en la naturaleza de los actores en conflicto como en los modos de acción propiciados, en gran medida, por los avances tecnológicos y por la evolución de las ideas. La innovación continuada se le denomina, en la Doctrina Conjunta española, *transformación*.

Las tres fechas con anterioridad expuestas, que históricamente cubren un brevísimo espacio de tiempo, son los hitos que marcan un camino de cambio en la forma de hacer la guerra, dentro de la continuidad de su naturaleza, aunque algunas veces se haya intentado negar el carácter permanente de ésta. La situación de las dos últimas décadas ha llevado a mitificar ciertos modos de acción, de efímera vigencia por cierto, que han servido para categorizar las percepciones de amenaza. Lo primero ha sido una constante en la historia militar, lo segundo tampoco es nuevo, pero nunca había sido tan publicado.

² GRAY, Colin S.: *War-Continuity in Change, Change in Continuity*, Parameters, US Army War College, Otoño de 2010.

En el ámbito de los fundamentos de la Doctrina Militar, en un espacio de 20 años se ha pasado, del auge del enfoque tecnológico con la *network-centric warfare*, la guerra del Golfo (1991) y su apogeo en Kosovo (1999), pasando por el no atendido aviso de Mogadiscio (1993). El patrón se cambió al iniciar la guerra de Afganistán (2001), pero volvió a repetirse en la invasión de Irak (2003) y ahí se paró el tiempo. Basándonos en estos hechos, en los estudios y adaptaciones doctrinales que se han efectuado, y en las lecciones de la Historia, se debe meditar como se puede enfrentar el futuro.

Para extraer lecciones de estas dos décadas debe admitirse, como una de las premisas básicas para cualquier análisis, que se han efectuado bajo la unipolaridad o hegemonía estratégica de Estados Unidos, que ellos han elegido la zona, el momento y el modo. De la misma forma, los modos de acción y el impulso doctrinal aplicado desde el mundo occidental en esta época, han sido, y son, de origen estadounidense.

El primer periodo (1990-2003) fue marcado por el desarrollo de la RMA (*Revolution in Military Affairs*), los conceptos de *shock and awe*, las armas guiadas, el sistema de ONA (*Operational Net Assessment*), etc., eran los instrumentos militares para controlar las operaciones en búsqueda de la situación final deseada establecida por la política. Era el paradigma de las Operaciones Basadas en los Efectos (EBO), el descubrimiento que permitiría disipar la «niebla» de la guerra. Las operaciones aéreas en Kosovo se vendieron como la prueba irrefutable de la viabilidad de las EBO. El estímulo era *top-down* en todos los aspectos. El EBO respaldó una cierta soberbia occidental: los problemas de la guerra tenían una solución que era cara en tecnología y barata en vidas, propias y ajenas. Esa «soberbia» es la que predispone a la política al abuso del empleo de las capacidades militares en cualquier circunstancia.

La situación cambió en el año 2003 cuando, una vez derrotado el Ejército iraquí y derrocado Sadam Hussein, la Administración americana y las fuerzas de la coalición se enfrentaron con una situación para el que no estaban preparadas doctrinal, anímica y materialmente. La falta de preparación doctrinal hizo que los neologismos que, tradicionalmente han servido para configurar la doctrina de una nueva época del arte militar, fueran sustituidos por antónimos para describir la situación e, incluso, los conceptos. Así, el empleo de términos tales como: asimétrico, no-convencional e irregular son muestra, además, de la impotencia conceptual con la que se ha enfrentado la situación.

El salto de la RMA a la COIN se efectuó mediante un impulso *botton up* impuesto por los acontecimientos. Antes de que el general Petraeus se hiciese cargo del mando en

Irak, muchos comandantes de Batallón y Brigada ya habían tenido que adoptar procedimientos de COIN sin indicaciones desde «arriba». En Irak fueron los mandos de nivel bajo y medio, los que identificaron las características del modo de hacer la guerra que se desarrolló tras la caída de Sadam Husein. Hicieron falta años de frustración, en palabras del general McKrystal³, para darse cuenta de que se enfrentaban a una estructura de red, y otros tanto para prepararse para ello. Hechos como Irak, Afganistán y antes Vietnam, demuestran que el cambio en la continuidad del modo de hacer la guerra lo impone la naturaleza de ésta, y el hecho de no captar la esencia del problema a enfrentar, ni de asimilar las enseñanzas del cambio se suele pagar, muy caro.

Adaptación

La adaptación, como respuesta al cambio, requiere la condición previa de tener la capacidad de percibirlo, valorar su incidencia y, en caso de juzgarse necesario, deducir un marco conceptual para afrontar la nueva situación. Este proceso, es eminentemente intelectual o, lo que es lo mismo, una tarea humana.

Para percibir el cambio se necesita tener conciencia de la situación, lo que incluye haber seguido su evolución. Sólo de esa forma se podrá teorizar sobre sus causas y ritmo, así como inferir la manera de poder reconducir los acontecimientos de manera que sean favorables a los intereses propios. La diferencia entre tener percepción del cambio o carecer de ella, se traduce en la menor o mayor probabilidad de ser sorprendido por los acontecimientos.

La explicación anterior puede ser considerada una obviedad, pero dejará de serlo en el momento que se imponga la sensación de ser superados por los acontecimientos. Las Fuerzas Armadas deben constituir un conjunto de capacidades versátiles, pero su empleo depende de la definición de la finalidad estratégica, del ambiente en que han de ser aplicadas y del adversario, y tener conciencia de ello es algo decisivo pues, en caso contrario, se corre un alto riesgo de emplear incorrectamente el instrumento militar y de caer en la derrota.

Como ya se ha indicado, la primera adaptación al cambio debe ser un impulso mental. La siguiente máxima de Carl von Clausewitz esclarece el asunto:

³ En: http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network

«El primero, el supremo, el más trascendente acto de juicio que un comandante debe efectuar es establecer... la clase de guerra en la que van a involucrarse; ni puede equivocarse ni convertirla en algo ajeno a su naturaleza.»

Parece que cuando escribió esto el prusiano estuviese pensando en las decisiones que se tomaron en Irak o Afganistán.

Lo anterior hay que ponerlo en relación con otro «aviso» «clauswitziano»

«... en la guerra, más que en cualquier otro asunto, debemos empezar mirando a la naturaleza del todo; porque aquí más que en cualquier otro asunto, la parte y el todo deben considerarse lo mismo.»

De aquí podemos deducir que la parte es la manera de hacer la guerra (*warfare*), «la clase de guerra», y, el todo, es la guerra (*war*) como fenómeno social.

Las anteriores reflexiones de Clausewitz demuestran que la aparición de lo que puede percibirse como nuevas e insospechadas formas de guerra no son nada nuevo; son parte de la naturaleza del fenómeno bélico. La percepción de cambio es el fundamento para la adaptación, pero no es suficiente; es necesario construir. El cambio hay que admitirlo como algo sustantivo no adjetivo, la situación resultante tiene su propia «naturaleza» como apunta Clausewitz y su gestión requiere, a su vez, modificar mediante la innovación.

Muchos son los que definen el actual, y previsible, ambiente estratégico como, complejo, impredecible y «no estructurado». No existe inconveniente en admitir esos calificativos, pero su enunciado no es suficiente para resolver el problema. Incluso tendrían efectos tóxicos si se empleasen como disculpas para justificar la inadecuación de las estructuras a la realidad. Hay que admitir los calificativos como descripción de la «normalidad», admitir la necesidad de evolución, actuar en consecuencia y aplicar procesos capaces de gestionar esa realidad, pues no hay otra.

Si el cambio es profundo respecto a los fundamentos de la Doctrina Militar al uso, hasta el punto que mediante su aplicación no puede alcanzarse la victoria, estamos ante un reto que necesita nuevos conceptos, incluso con una semántica propia. No debe haber temor a la habilitación de neologismos. Si, al contrario, para gestionar una situación de este tipo se opta por aplicar los antónimos del lenguaje propio de la situación anterior, estaremos ante un claro indicio de que no se comprende: «la clase de guerra en la que va a involucrarse (el comandante).»

Como ejemplo del problema valoremos el calificativo «asimétrico» para referirse a una amenaza. La simetría necesita una referencia, un «eje». Ese eje, en este caso, sirve para

comparar medios, cantidades, procedimientos, etc., pero siempre desde la referencia del que adjudica el adjetivo, que es el mismo que establece el «eje». Si la imagen no coincide con la propia, al enemigo se le atribuye la naturaleza de «asimétrico», a la que se llega no por el estudio de sus potencialidades, sino por la constatación del hecho de si se adapta o no al eje de simetría mental que nos caracteriza. Esta manera de afrontar el cambio es sintomática de un error de juicio en la valoración de la situación y la subsiguiente incapacidad para la adaptación, pues se parte de una pretendida superioridad del conocimiento y de otros juicios de valor como de inadecuaciones del contrario al no ser como «nosotros» o que «ellos» están fuera de la ortodoxia al uso. Ese es el estado mental que nos lleva a describirlo como irregulares, no-convencionales, asimétricos, insurgentes, etc. Es el triunfo de la traición del subconsciente.

Otro aspecto a tener en cuenta es el empleo de términos imprecisos para definir los fundamentos de nuestra actuación. Si definimos el ambiente estratégico como «no estructurado», estaremos renunciando de antemano a «estructurar» nuestras reacciones. Cuanto más intensamente contemplemos la realidad como «no estructurada», debemos ser más conscientes de que padecemos un mayor retraso en el cambio. La realidad es la que es y necesita de la estructuración de nuestras mentes para su gestión, no al revés. Si no se admite este hecho, no existirá mentalidad de adaptación, de cambio.

La adaptación tiene su origen natural en el ámbito estratégico o, lo que es lo mismo, debe ser un proceso *up-down* porque tiene que ser liderada desde la convicción del que va a efectuar «el más trascendente acto de juicio». Ese «acto de juicio» debe incluir la evaluación del adversario en cuanto a finalidad estratégica, modos, medios y fines, desde el ángulo de su idiosincrasia. Es la puesta en práctica del aforismo de Sun Tzu: «Conoce al adversario, concóctete a ti mismo y ganarás...»

Desde aquí es desde donde debería considerarse la amenaza. El enemigo se adaptará a sus posibilidades, a las capacidades que brinda la tecnología, al ambiente y a la finalidad a alcanzar. Desde esta óptica, la amenaza viene conformada por el actor antagonista, porque el actor es el único que es capaz de diseñar los modos de aplicación de los medios y de ejercer la voluntad de aplicarlos.

Lo anterior parece contradecir el uso cotidiano del empleo del vocablo amenaza. Así se habla de la amenaza terrorista, la amenaza del narcotráfico o la amenaza de los vehículos aéreos no tripulados. El «abuso» del término, en ámbitos profesionales, llega a difuminar la diferencia entre los dominios estratégico, operacional y táctico y esta circunstancia está en el origen de errores de planeamiento y ejecución. Por ejemplo, al hablar de la amenaza

terrorista, o cibernética, nos referimos a modos. En el primer caso, el denominado terrorismo, que es una acción táctica que produce efectos estratégicos, afectando a las capacidades del contrario desde una perspectiva psicológica, al tener una difusión mediática muy amplia, desde diferentes puntos de vista, lo que actúa como impulsor para modular percepciones. En este caso la acción terrorista no debería considerarse como amenaza, porque sería sustantivar un modo de acción, el actor que emplea el terrorismo es la amenaza.

La primera década del presente siglo ha retribuido a las Fuerzas Armadas con el problema de tener que prepararse para hacer frente a una multiplicidad de amenazas y, ese hecho, les obligará a reestructurarse en un contexto, previsiblemente, de penuria presupuestaria. Uno de los peligros a que tendrá que enfrentarse este proceso es el caer en la simplificación mediante el dilema de la elección entre opciones, por ejemplo, entre COIN o «convencionalismo». Este hecho tiene poco que ver con la adaptación, en su sentido general, más bien a la «acomodación» a un determinado escenario. La tendencia a la simplificación no debe conducir al simplismo, pero de ella puede inferirse un primer corolario: para ambientes complejos de seguridad, donde es muy alta la incertidumbre respecto al futuro carácter de la guerra, hay que habilitar flexibilidad operacional. La necesidad de adaptación puede que padezca evidente, pero cómo hacerlo es la cuestión.

Muchos son los que definen el actual, y previsible, ambiente estratégico como, complejo, impredecible y «no estructurado». No existe inconveniente en admitir esos calificativos, pero no son suficientes para resolver el problema. Incluso tendrían efectos tóxicos si se empleasen como disculpas para justificar la inadecuación de las estructuras a la realidad. Hay que admitir los calificativos como descripción de la «normalidad», actuar en consecuencia y aplicar procesos capaces de gestionar la realidad, pues no la realidad no se puede sustituir por la narrativa al uso.

Innovación

La adaptación como solución a un problema, debe contar con elementos que permitan traducir a hechos lo que en principio no deja de ser una mera visión. El ejercicio del liderazgo es el origen de la creación de los elementos materiales que permitan la adaptación al cambio: la innovación. Liderar es una actuación subjetiva y, por lo tanto, entraña un juicio de valor. La necesidad de innovar, como vehículo para la adaptación, puede que se vea cómo evidente, pero una cosa es decirlo, incluso estar convencido de ello, y otra llevarlo a cabo. De esta forma, la innovación, se presenta tanto como un fin

como un proceso. La primera acepción es relativamente fácil de asimilar si se cuenta con la suficiente perspicacia para ello, la segunda es la que se pretende tratar a continuación.

Al considerar todo lo relacionado con la innovación militar, o transformación, habrá que enmarcar nítidamente de que se está hablando. Cuando se diseñan y constituyen las capacidades militares de una nación, no se está simplemente ante un proceso de gestión de recursos, es una tarea más compleja, en la que juegan factores políticos, culturales e institucionales. La actuación de estos factores, normalmente, crea una dinámica de sentido contrario a los impulsos de cambio. Estas consecuencias son extraídas de la Historia y formarán parte, de forma natural, de cualquier «paisaje» de cambio que se afronte.

Habrá quien objete que la innovación ha existido siempre, y es cierto. En el mismo sentido también habrá que admitir que la mayoría de las innovaciones han ido de la mano de avances tecnológicos. Quien ha poseído la ventaja tecnológica, y ha previsto correctamente como utilizarla, ha marcado el camino. Pero esa es una versión retrospectiva de los hechos, una constatación del pasado. El problema se nos presenta, como es el caso, cuando la innovación se constituye como parte esencial de la actividad militar, un reto de futuro, como un requisito ineludible para la institución que tiene a su cargo la defensa de la supervivencia de la entidad política. Esto podía expresarse gráficamente citando al general Peter Chiarelli (*US Army*), que dijo que era importante que las duras lecciones de Irak y Afganistán no sean sólo «conocidas», sino realmente «aprendidas», incorporadas en el DNA del Ejército y en la memoria de la institución⁴.

La innovación del pasado, normalmente, se conformaba como una reacción a situaciones determinadas, presentes, tales como: coraza contra potencia de fuego, fortificación *versus* maniobra, poder aéreo ofensivo contra defensivo, etc. siempre en un sentido absoluto de progreso. Por el contrario la necesidad actual de innovación viene determinada por la concurrencia, en conflicto, de factores tales como actores de diferente naturaleza (Estados y organizaciones no estatales), conectividad global, acceso universal a la mayoría de las tecnologías, reacciones a estímulos mediáticos evanescentes, etc.

La actual necesidad de innovación permanente es consecuencia de la existencia de amenazas, o potencial de ellas, la mayoría de las veces no mensurables en entidad, dirección y, lo que es más difícil de percibir, de naturaleza novedosa, y esa novedad no siempre está orientada hacia lo que se considera normalmente como progreso, sino que

⁴ Aludido por el secretario de Defensa Robert Gates en su discurso en la Academia Militar de West Point, 25 de febrero de 2011, en: <http://www.defense.gov/speeches/speech.aspx?speechid=1539>

muchas de estas amenazas contienen elementos primitivos. Para las Fuerzas Armadas, la innovación, constituye un reto para su supervivencia pues la agilidad buscada va a encontrarse con un enemigo institucional correoso y sólido: la burocracia.

La institucionalización de la innovación como parte integral del «quehacer» militar, presenta para las Fuerzas Armadas varios riesgos en relación con este hecho. Uno de ellos es de carácter negativo, la inacción, no asimilar institucionalmente que constituye una necesidad ineludible, lo que llevaría a enrocarse en postulados obsoletos, a la irrelevancia de la organización militar, por inadecuada al ambiente en que tiene que actuar. Otro, e igual de grave, es la sobreactuación, lo que produciría un dispendio de energías y recursos sin retribución alguna, a la vez que a una frustración que bloquearía la creatividad necesaria. Todo ello nos lleva a la necesidad de que este proceso, como todos los militares, necesite liderazgo.

La innovación no debe gestionarse como una actividad futurista ni como un conjunto de simples experimentos. La referencia para el cambio tendrá que proceder de una continua evaluación de la situación estratégica que se orientaría a la identificación de hechos (*drivers*) productores de efectos que conforman tendencias de futuro y a la identificación de las mismas. En este punto es importante poner de manifiesto que no se trata de adivinar el futuro, eso constituiría una vulneración flagrante de la aplicación del conocimiento; el futuro, por definición, no puede conocerse, pero puede prepararse.

Si algo han puesto de manifiesto las guerras de Irak y Afganistán es que la tecnología, por sí sola, no puede gobernar la innovación. Es, en todo momento, la finalidad del proceso el timón de la actividad. Los ataques del 11 de septiembre de 2001 por parte de Al Qaeda, emplearon el estado de la tecnología para efectuarlos y confiaron al poder mediático la explotación estratégica, pero no pretendían la destrucción material de Estados Unidos, sólo su desequilibrio estratégico, alienando al mundo musulmán, empeñando a las fuerzas americanas en Asia y «fabricando» un enemigo de Estados Unidos tras el que se reuniese el mundo musulmán. Las ideas mandan, éste es uno de los elementos primitivos de la actual situación, y la formación de los componentes de la fuerza conjunta, a todos los niveles, se presenta como un requisito esencial de la eficacia de dicha fuerza. La identificación de problemas y la creación de conceptos requieren mentes ágiles en los puestos de dirección, en este sentido, la formación permanente de los oficiales es de la mayor importancia.

La innovación debe de incluir los fundamentos relacionados con la economía en su sentido técnico: la asignación de medios escasos, susceptibles de usos alternativos, a

diversas necesidades. En una época de recursos escasos y conflictos permanentes, la «economía» se erige en referencia permanente. La sinergia entre organización, tecnología y procesos será la forma de obtener eficiencia, ahí está el reto. El proceso de innovación requiere, para su funcionamiento, la inversión de recursos que habrá que extraer de otras actividades, de aquellas que no promuevan la eficiencia. El adelgazamiento de estructuras es un requisito de futuro.

Amenazas y semántica

La percepción general es que lo relacionado con aquello que antes se consideraba el quehacer estratégico ha pasado a ser tarea relacionada con la opinión publicada que, a falta de fundamentos más sólidos, se erige en el elemento básico en la toma de decisiones. De igual modo, la semántica empleada por los medios infecta el ámbito profesional, induciendo a confusión intelectual en el ámbito militar. La asimilación en el ámbito profesional de términos periodísticos resta precisión al lenguaje profesional, lo que se traduce en una creciente pobreza doctrinal. La inclusión de las denominadas «operaciones de paz» en la Doctrina Militar, en la última década del siglo XX, dejaron vacío de contenido estratégico el empleo de la fuerza militar. Una semántica confusa tiene consecuencias perversas.

La percepción de amenazas se deriva del conocimiento de las capacidades de los enemigos, o potenciales enemigos, en relación con las vulnerabilidades de los objetivos que materializan nuestros intereses. En principio partimos del ámbito de las percepciones, lo que otorga a la definición de las amenazas un alto grado de subjetivismo.

Anteriormente se ha expuesto el riesgo que asumimos al confundir modos de actuación con el enemigo e, incluso, con el fenómeno bélico. Esta confusión va de la mano de una semántica que, mediante la amplificación mediática, produce los efectos indeseados. Recordemos durante la guerra fría, la amenaza la constituía el Pacto de Varsovia, no sus divisiones acorazadas ni los submarinos soviéticos. Las fuerzas de la Organización del Tratado del Atlántico Norte (OTAN) se articulaban para hacer frente a lo que se derivaba del *risk assessment*. Después de la guerra fría la cosa derivó por diferentes derroteros.

Como ya se ha indicado anteriormente, después de los ataques del 11 de septiembre de 2001 a Estados Unidos se acuñó el término GWOT con lo que se le dio carta de naturaleza a la acción sobre la amenaza. La acusación que se le hace al presidente Bush por ello, es que al centrarse la atención en el terrorismo en vez de hacerlo sobre Al Qaeda, o el islamismo radical, se elevó un modo de acción, la actuación táctica para crear

terror, al fundamento para articular toda una opción estratégica, lo que desenfocó el esfuerzo estratégico de Estados Unidos, circunstancia que dura hasta ahora.

Esto nos lleva a constatar que el mal se inserta en las instituciones. Cuando una de ellas emplea oficialmente la denominación de amenaza fuera de su contexto, se promueve la confusión, como es el caso de la OTAN con la denominada «amenaza híbrida». Se trata de enunciar el empleo de varios modos de acción en un determinado contexto de conflicto, incluyendo procedimientos «convencionales», acciones terroristas, ciberguerra, acciones criminales, etc.

La inclusión del término «amenaza» en un documento doctrinal de la Alianza presenta, en primer lugar, la duda de cuál es el ámbito de la misma: a la Alianza como un todo, a sus fuerzas en operaciones, a sus poblaciones, etc. Hay que insistir en que la amenaza es el actor que emplea esos modos de acción, no los modos. En el caso concreto de la «amenaza híbrida» puede identificarse perfectamente con la que realmente constituye *Hizbollah* para Israel, esa es la amenaza para el Estado judío, no los procedimientos «híbridos».

La preparación de la fuerza conjunta debe efectuarse al margen de estas disquisiciones y alistarse para actuar en conflictos donde la amenaza proceda de actores estatales y no estatales que emplearán una amplia panoplia de medios. Las novedades provendrán de los ámbitos donde se desarrollará en conflicto, ya que la tecnología habilita nuevos espacios y esa circunstancia lo que nos indica que hay que adaptarse. La Estrategia Militar de Estados Unidos⁵ da un claro aviso al incorporar importantes novedades en cuanto a ámbitos de actuación.

Aunque parezca reiteración, habrá que admitir que nos adentramos en una época de multipolaridad económica, de actores estratégicos de diferente naturaleza, de modos de acción diversos y de conflicto permanente. Las novedades más importantes son aquellas que se derivan de la habilitación de dos nuevos ámbitos de *warfare*: el espacio exterior y el ciberespacio. Esa circunstancia es básica para articular los modos de acción militares.

Aspecto importante es no adoptar una actitud de estar ante una realidad virtual. La red talibán utiliza teléfonos vía satélite para coordinar sus operaciones. Se aprovecha del uso del espacio exterior que habilitan Estados Unidos para llevar a cabo operaciones contra las fuerzas estadounidenses. Si los talibán fuesen capaces de actuar en ese ámbito para afectar las comunicaciones de las fuerzas aliadas, el «destrazo» sería de altas

⁵ *The National Military Strategy of The United States*, Department of Defence, Washington, febrero de 2011.

proporciones. Seguro que a ningún profesional se le ocurriría pensar que en esta situación se está ante amenazas «asimétricas».

A partir de ahora, el empleo de los dominios cibernético y espacial hay que considerarlos como «normalidades» que pueden emplearse tanto en modo ofensivo como defensivo, a la vez que verlos como *enablers* para la actuación en los otros tres dominios: terrestre, marítimo y aéreo. El hecho de la introducción de esta novedad en la Estrategia Militar de Estados Unidos es un ejemplo de aceptación del cambio, un esfuerzo de adaptación y una guía para la innovación.

Estos «condicionantes» entran de lleno en los fundamentos en que se basan las Fuerzas Armadas actuales y España no puede ser una excepción. En un tiempo convulso y confuso, como el que nos ha tocado vivir en estos comienzos del siglo XXI, la responsabilidad de los militares es creciente. Ésta no se circunscribe a mantener en perfecto «estado de revista» a las Fuerzas Armadas, se extiende a la previsión en una panoplia de ámbitos que van desde la prospectiva estratégica, a los avances tecnológicos, aspectos culturales y un largo etcétera.

Los retos a los que se enfrentará la fuerza conjunta no requerirán el empleo de una semántica extravagante. El ejercicio de las actividades de disuasión, el mantenimiento expedito de las rutas marítimas, la destrucción de focos de actividades agresivas, la entrada en fuerza en zonas hostiles, la lucha contra medios de lanzamiento de armas de destrucción masiva, la neutralización de acciones ofensivas, serán, entre otras algunas de sus actividades. A estos retos habrá que agregar el que representa el ambiente creado por las narrativas, que determinará el sesgo de la opinión pública y, por lo tanto, será un factor que influirá en las operaciones.

Este desafío es ante todo un reto al empleo del conocimiento. El asesoramiento militar a quienes deben de tomar la decisión política es un asunto que necesita de gran preparación por parte del que lo proporciona. Preparación, que en este caso no es sinónimo de falta de agilidad u oportunidad, sino de anticipación consciente. Con todo, la naturaleza del ambiente estratégico, los efectos de la política y las naturales resistencias de la institución militar al cambio, conformarán una clase de «fricción» tan perniciosa como a la que se refería Clausewitz.

En una época donde la opinión pública, principal servidumbre del poder político, y la «lógica» de los expertos militares no coinciden, es difícil llegar a conseguir el apoyo de aquélla, que es un requisito necesario para la victoria. La forma de conseguirlo es política y, por lo tanto, es labor de los políticos revertir la situación. Para ello, el camino no pasa

por que la institución militar incorpore en su esencia profesional los elementos de los mensajes mediáticos ni los usos de la política, sino que mantenga la especificidad de su ámbito profesional. El decidir el empleo de la fuerza militar es asunto de la política, el cómo hay que hacerlo es objeto de la profesión militar.

ENRIQUE FOJÓN LAGOA
Coronel de Infantería de Marina (R)

LA EVOLUCIÓN DEL PARADIGMA ESTRATÉGICO OCCIDENTAL EN EL MUNDO GLOBALIZADO

Introducción

En las páginas anteriores, Enrique Fojón Lagoa ha analizado la evolución del marco estratégico internacional y la transformación de la amenaza desde el fin de la guerra fría hasta la actualidad. Para ello, se ha valido de tres grandes hitos que han supuesto un punto de inflexión en la historia reciente: la caída del muro de Berlín el 9 de noviembre de 1989, que terminó con el orden internacional bipolar; los ataques terroristas contra Estados Unidos el 11 de septiembre de 2001, que acabaron con la aparente pausa estratégica que estaba viviendo el mundo desde el fin de la guerra fría; y finalmente la quiebra del banco de inversión Lehman Brothers el 15 de septiembre de 2008, que reveló la fragilidad del sistema financiero internacional y el comienzo de una nueva etapa marcada por la escasez de recursos y la incertidumbre estratégica.

La presente contribución también tomará como base estos tres hitos históricos con el objeto de analizar las concepciones estratégicas y las políticas de seguridad y defensa el mundo occidental desde el fin de la guerra fría hasta la fecha de hoy; y cómo éste ha identificado los riesgos y las amenazas a la paz y la seguridad internacional. Así, se observará como la caída del Telón de Acero terminó con el peligro de desatarse una conflagración global entre las dos superpotencias, abrió las puertas a una revolución militar que se había estado gestando en los años anteriores, comportó el cobro del «dividendo de la paz» e implicó una creciente participación de las Fuerzas Armadas en operaciones de mantenimiento de la paz.

Diez años después, los ataques sobre Nueva York y Washington terminaron con la aparente estabilidad que estaba viviendo el mundo de la posguerra fría, revelaron algunos de las nuevas amenazas a la seguridad global, urgieron a los países a transformar sus entramados de seguridad y defensa para adaptarlos al nuevo marco internacional y las campañas afgana e iraquí pusieron de manifiesto las cualidades y límites del modelo militar vigente hasta la fecha y revelaron el cambiante rostro de la guerra. Finalmente, la crisis económica global ha coincidido con el reconocimiento del empantanamiento de los

conflictos afgano e iraquí, la constatación de los ingentes costes políticos, militares, estratégicos, sociales y económicos que entraña la participación en largas e indefinidas campañas, y la entrada en un nuevo marco estratégico caracterizado por la escasez de recursos y la incertidumbre con el objeto de satisfacer un creciente número de necesidades y superar un mayor volumen de contingencias.

El pensamiento estratégico occidental en la inmediata posguerra fría

El primer punto de inflexión estratégico en nuestra historia reciente se produjo con la caída del Telón de Acero, puesto que el fin del mundo bipolar supuso el desvanecimiento de los dos principales pilares militares de la guerra fría –la disuasión nuclear y las grandes unidades– y comportó la reestructuración de las políticas de seguridad y defensa de los países avanzados¹. Y es que mientras desaparecía la amenaza sobre la que éstos habían construido sus arquitecturas defensivas y la aparente estabilidad global permitía reducir tanto su gasto militar como cobrar el «dividendo de la paz», también empezaban a vislumbrarse nuevos peligros de distinta naturaleza, intensidad y procedencia que aconsejaron ampliar el concepto de seguridad más allá de la tradicional defensa del territorio².

Y es que el peligro de desatarse una tercera guerra mundial, contemplado como factible hasta entonces, dejó paso a un mundo en el que se combinaban riesgos y amenazas tan dispares como los “Estados fallidos”, “débiles” o en “descomposición”, las catástrofes ambientales, los movimientos migratorios incontrolados, las crisis humanitarias, el terrorismo internacional, la criminalidad transnacional o la proliferación de armamento de destrucción masiva. En otras palabras, la guerra fría estaba dejando paso a un nuevo orden internacional que terminaría revelándose muy distinto al imaginado por Francis Fukuyama en plena euforia poscomunista³.

Pronto estallaron nuevas crisis que precisaron una respuesta de la comunidad internacional y revelaron algunos de los nuevos requerimientos que debían satisfacer las Fuerzas Armadas de Occidente. No sólo debían de ser capaces de responder rápidamente a muchas y muy variadas crisis que pudieran surgir en cualquier punto del globo; sino que una vez allí debían poder realizar, de forma autónoma o en un ambiente multinacional e interagencias, una gran variedad de misiones (desde ayuda humanitaria,

¹ DYSON, Tom: *Neoclassical Realism and Defence Reform in Post-Cold War Europe*, Palgrave MacMillan, Londres, 2010.

² CLARKE, Michael (ed.): *New Perspectives on Security*, Brassey's, Londres, 1993 o FISCHER, Dietrich: *Nonmilitary Aspects of Security. A Systems Approach*, Dartmouth Publishing, Aldershot, 1993.

³ FUKUYAMA, Francis: *The End of History and the Last Man*, The Free Press, Nueva York, 1992.

pacificación, estabilización, contrainsurgencia hasta guerra convencional) contra adversarios muy diversos (ejércitos regulares, guerrillas, señores de la guerra o grupos terroristas), en todo tipo de ambientes (urbanos, montañosos, desiertos o selváticos) y en un marco más complejo y confuso que en el pasado, donde factores ajenos a los militares (legales, sociales, políticos, humanitarios o mediáticos) no sólo podían condicionar el curso de la misión, sino determinar su desenlace⁴.

En consecuencia, los ejércitos occidentales –equipados, organizados y adiestrados para defender el territorio europeo frente una invasión del Pacto de Varsovia– no sólo debían prepararse para un mayor número de contingencias; sino que también tenían que reducir y reestructurar su potencial humano y material para adaptarse a la disipación de la amenaza soviética, el fin de la conscripción universal y el cobro del «dividendo de la paz».

A pesar de la trascendencia de estos asuntos, durante la inmediata posguerra fría los debates en la esfera de la seguridad y la defensa se articularon en torno a temas como la crisis del vínculo trasatlántico, las operaciones de paz o las nuevas concepciones de seguridad; y eran muy pocos los estrategas que se aventuraron a plantear seriamente cómo serían los conflictos futuros⁵. En este sentido, es muy probable que la aparente paz reinante en el globo junto con la inexistencia de una amenaza concreta y definida motivaran este relativo abandono del análisis estratégico y reforzaran la creencia de que el mundo había entrado en una etapa de paz y estabilidad que se dilataría hasta bien entrado el siglo XXI⁶. Por lo tanto, no es extraño que en este vacío estratégico, la idea de una Revolución en los Asuntos Militares (RMA) motivada por la aplicación militar de las tecnologías de la información y capaz de transformar el arte de la guerra, articulara el debate estratégico internacional hasta los trágicos sucesos de septiembre de 2001⁷.

Originada tras la derrota estadounidense en Vietnam para terminar con el frágil equilibrio del terror reinante en Europa durante los años setenta, estudiada secretamente en las más altas esferas de Washington y de Moscú durante los años ochenta y

⁴ PÉREZ, Jesús M.: *Guerras Posmodernas*, Ediciones el Cobre, Barcelona, 2010 o CREVELD, Martin van: «Through a Glass, Darkly: Some Reflections on the Future of Warfare», *Network-Centric Warfare Review*, pp. 25-44, otoño de 2000.

⁵ Véase, por ejemplo, SULLIVAN, Gordon R. y DUBIK, James M.: *War in the Information Age*, U.S. Army Strategic Studies Institute, Carlisle Barracks, 1995; ARQUILLA, John y RONFELDT, David (eds): *In Athena's Camp: Preparing for War in the Information Age*, RAND Corporation, Santa Monica, 1997 o CREVELD, Martin van: *The Transformation of War*, The Free Press, Nueva York, 1991.

⁶ METZ, Steven: *Armed Conflict in the 21st Century: the Information Revolution and Post-Modern Warfare*, U.S. Army Strategic Studies Institute, Carlisle Barracks, 2000.

⁷ En términos generales, una RMA es un profundo cambio en la forma de combatir que resulta de la integración de nuevas tecnologías, conceptos operativos o formas de organización en las fuerzas armadas. Esta transformación convierte en irrelevante u obsoleto el estilo militar pre-revolucionario y proporciona una enorme superioridad al primer ejército que explota estas capacidades. Es por ello que todos sus posibles adversarios deberán alcanzar este nuevo estándar de capacidades, bien sumándose a la revolución o desarrollando una respuesta susceptible de acabar con esta ventaja. COLOM, Guillem: *Entre Ares y Atenea, el debate sobre la*

popularizada mundialmente tras la espectacular victoria aliada en la guerra del Golfo del año 1991⁸; esta revolución prometía victorias rápidas, decisivas y sin apenas daños colaterales en toda la gama de las operaciones gracias al empleo de una fuerza conjunta muy tecnificada y con un total conocimiento del entorno operativo⁹. Estas características parecían hacer de la RMA la solución perfecta a todos los problemas estratégicos que debían superar las sociedades avanzadas de fin de siglo: la erosión del modelo de ciudadano-soldado y el fin de la conscripción universal masculina, la disminución del gasto en defensa provocado por la disipación de la amenaza, la creciente participación en operaciones de gestión de crisis y apoyo a la paz, la necesidad de conservar la supremacía militar frente a adversarios futuros, y muy especialmente, parecía enmendar la creciente dificultad de las sociedades posheroicas para recurrir a la guerra como instrumento político¹⁰.

En consecuencia, no es de extrañar que esta revolución sedujera a políticos y militares de todo el mundo puesto que no sólo prometía reemplazar la menor disponibilidad de efectivos humanos y recursos financieros con tecnología; sino que ofrecía a los gobiernos occidentales la posibilidad de continuar empleando la fuerza armada como elemento de política exterior con unos costes políticos, económicos y sociales perfectamente asumibles por sus opiniones públicas.

Paralelamente, expertos de todo el mundo se apresuraron en determinar las características fundamentales de esta revolución y sus potenciales efectos sobre el arte de la guerra. Así, observaron que su esencia radicaba en el «sistema de sistemas» o la capacidad que tendría cualquier sensor, plataforma, combatiente o arma para interactuar con el resto gracias a su integración en red. Ello proporcionaría un total conocimiento del campo de batalla y permitiría que una fuerza conjunta geográficamente dispersa batiera con plena precisión cualquier objetivo a gran distancia y sin apenas daños colaterales¹¹. Tal posibilidad sentaría las bases de la guerra en red (*network centric warfare*), considerada como el estilo de guerra propio de la Era de la Información¹².

Revolución en los Asuntos Militares, Instituto Universitario General Gutiérrez Mellado-Universidad Nacional de Educación a Distancia (UNED), Madrid, 2008.

⁸ KAGAN, Frederick W.: *Finding the Target: The Transformation of American Military Policy*, pp. 7-76, Encounter Books, Nueva York, 2006.

⁹ SCHNEIDER, Barry R. y GRINTER, Lawrence (eds.): *Battlefield of the Future*, Maxwell, Air University Press, 1988.

¹⁰ MOSKOS, Charles; WILLIAMS, James y SEGAL, Don: *The Post-Modern Military: Armed Forces after the Cold War*, Oxford University Press, Nueva York, 2000.

¹¹ OWENS, William A.: «The Emerging System-of-Systems», *U.S. Naval Institute Proceedings*, volumen 121, número 1.105 pp. 35-39, mayo de 1995.

¹² ALBERTS, David S.; GARSTKA, John J. y SEIN, Frederick: *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Press, Washington D.C., 1999.

Y para conquistar la RMA, juzgaron esencial adquirir las novedosas tecnologías propias de la Era de la Información (modernas plataformas furtivas, avanzados sensores de Mando, Control, Comunicaciones, Computadores, Inteligencia, Vigilancia, Adquisición de Blanco y Reconocimiento (C⁴ISTAR) y sofisticadas armas inteligentes integradas en red creando un sistema de sistemas)¹³; desarrollar nuevas formas de actuación (acción conjunto-combinada, operaciones basadas en efectos, rápidas y decisivas, orientación expedicionaria y guerra espacial, ciberespacial e informativa); aplicar nuevos modelos de organización (adelgazamiento y racionalización de estructuras, generación de fuerzas modulares, altamente desplegadas y preparadas para combatir en toda la gama de operaciones); implantar nuevas competencias (nuevos modelos de adiestramiento, mayores responsabilidades y nuevos cometidos) e implementar nuevos estilos de conducción de las operaciones militares (descentralización del mando, nueva organización de los estados mayores, mayor control estratégico y político de las operaciones o integración de la cadena de mando militar bajo control civil en operaciones interagencia)¹⁴. Este conjunto de cambios en la estructura, equipamiento, organización y funcionamiento de las Fuerzas Armadas con el objeto de alcanzar la RMA pasaron a fundamentar el proceso de planeamiento estratégico de Occidente durante la década de los años noventa¹⁵.

Resumiendo, mientras el estudio de la RMA, la identificación de sus características definidoras y la evaluación de sus potenciales efectos sobre el arte de la guerra constituyeron los grandes ejes sobre los que se articuló el pensamiento estratégico de Occidente durante la inmediata posguerra fría; la conquista de la revolución y la generación de un nuevo catálogo de capacidades universalmente aplicable a toda la gama de operaciones presentes y futuras lo hicieron sobre su planeamiento de la defensa. Este proceso enfocado a lograr la RMA y desarrollar un conjunto de capacidades militares adecuadas para las guerras futuras recibió el nombre de *transformación*¹⁶. No obstante, debería esperarse hasta el 11 de septiembre de 2001 para que este proceso se

¹³ FRIEDMAN, George y Meredith: *The Future of War: Power, Technology and American World Dominance in the Twenty-First Century*, St. Martin's Griffin, Nueva York, 1998.

¹⁴ LIPPITZ, Michael y WHITE, John P. (eds.): *Keeping the Edge: Managing Defense for the Future*, The MIT Press, Cambridge, 2001.

¹⁵ LOO, Bernard (ed.): *Military Transformation and Strategy: Revolutions in Military Affairs and Small States*, Routledge, Londres, 2008.

¹⁶ ROXBOROUGH, Ian: «From Revolution to Transformation, the State of the Field», *Joint Forces Quarterly*, número 32, pp. 68-76, otoño de 2002..

convirtiera en un imperativo estratégico para adaptar los ejércitos modernos al mundo del tercer milenio¹⁷.

En conclusión, durante la inmediata posguerra fría el pensamiento estratégico y el planeamiento de la defensa se articularon en torno a la RMA, una revolución que parecía constituir la respuesta a todos los interrogantes estratégicos que debían responder las sociedades avanzadas de fin de siglo. Posibilitada por las tecnologías de la información, basada en la obtención del pleno conocimiento del campo de batalla y configurada en torno a la generación de pequeñas fuerzas conjunto-combinadas dominando las esferas terrestre, marítima, aérea, espacial, ciberespacial e informativa para lograr victorias rápidas, decisivas, limpias y sin apenas daños colaterales, esta RMA parecía ser la culminación de la guerra convencional.

Y es que si bien esta revolución pretendía confeccionar un catálogo de capacidades militares apropiado para actuar en toda la gama de operaciones y derrotar cualquier potencial adversario presente o futuro, en general se asumía que ésta serviría para incrementar la brecha de capacidades militares convencionales entre Occidente y el resto del globo¹⁸. En este periodo de fervor revolucionario, fueron muy pocos los estrategas que alertaron de la excesiva confianza puesta en la tecnología, las posibles limitaciones de la RMA en escenarios irregulares o las incógnitas que suscitaba este nuevo estilo de combatir a tenor de las experiencias en Somalia o los Balcanes.

Convencidos de que cualquier aliado o competidor de Occidente intentaría conquistar esta revolución, solamente tomaron en consideración la respuesta asimétrica que propusieron dos oficiales de la República Popular China¹⁹. Concedores de la imposibilidad de su país para lograr la RMA, éstos sugirieron emplear acciones de guerra sin restricciones –utilización de armamento de destrucción masiva, actos terroristas indiscriminados, ciberguerra, ataques contra los flujos financieros y las redes de información y comunicaciones, manipulación de las opiniones públicas o guerra legal– para anular la supremacía militar de Occidente. Sin embargo, en este periodo marcado por la ilusión tecnológica, prácticamente ningún estratega podía imaginar que una forma de lucha a priori tan arcaica y simple como la guerra irregular revelaría los límites del estilo militar posrevolucionario²⁰.

¹⁷ FREEDMAN, Lawrence: «The Transformation of Strategic Affairs», *Adelphi Paper*, número 379, Oxford University Press, Londres, 2006.

¹⁸ SLOAN, Elinor: *The Revolution in Military Affairs*, McGill-Queen's University Press, Montreal, 2002.

¹⁹ LIANG, Quiao y XIANGSUI, Wang: *La guerre hors limites*, Rivages, París, 2004.

²⁰ LUTTWAR, Edward, N.: «A Post-Heroic Military Policy», *Foreign Affairs*, volumen 75, número 4, pp. 33-44, julio-agosto, 1996.

Posiblemente, si los estrategas occidentales no hubieran caído en este espejismo tecnológico y hubieran observado con mayor atención la evolución del entorno de seguridad global y la naturaleza de los conflictos que habían surgido tras la caída del Telón de Acero, con toda probabilidad éstos habrían moderado sus proclamas revolucionarias y no se habrían visto sorprendidos por los acontecimientos de Afganistán o Irak, tal y como finalmente sucedió pocos años después.

El imperativo estratégico y la guerra contra el terror

Los ataques del 11 de septiembre de 2001 contra las ciudades de Nueva York y Washington constituyen el segundo de los hitos de nuestra historia reciente. Éstos acabaron con la pausa estratégica iniciada tras la caída del Telón de Acero y supusieron «...el retorno de la historia y el fin de los sueños»²¹ al revelar algunos de los nuevos riesgos y amenazas a la seguridad global y acabar con las proclamas revolucionarias de la década anterior.

Aunque esta segunda etapa arrancó formalmente en septiembre de 2001, sus fundamentos ya se habían establecido varios meses antes, coincidiendo con la llegada de George W. Bush a la Casa Blanca²². Cautivado por el potencial de la RMA y consciente del papel que ésta tendría en la configuración del nuevo orden mundial, el presidente Bush y su secretario de Defensa Rumsfeld trazaron un ambicioso proceso de *transformación* para conquistar rápidamente la revolución y preparar la arquitectura de seguridad y defensa estadounidense para satisfacer con éxito los retos que el país debería afrontar en el año 2020, que era supuestamente el año en que terminaría esta larga pausa estratégica iniciada en el año 1991. Para tal fin, no sólo formularon una nueva política de seguridad, defensa y militar adecuada al entorno estratégico de la posguerra fría; sino que situaron la *transformación* del entramado de defensa del país –desde la estructura, volumen, equipamiento y capacidades de sus Fuerzas Armadas hasta la organización, funcionamiento, administración y financiación del Pentágono– como una de las principales prioridades políticas de la nueva administración republicana²³.

Aunque en un primer momento esta propuesta tuvo un enorme impacto entre la comunidad estratégica estadounidense y limitados efectos en el resto de unas potencias

²¹ KAGAN, Robert: *The Return of History and the end of Dreams*, Knopf Publishers, Nueva York, 2008.

²² KITFIELD, James: *War & Destiny: How the Bush Revolution in Foreign and Military Affairs Redefined American Power*, Potomac Books, Washington D.C., 2005.

²³ A tal efecto, véase la lectura del programa de defensa del flamante inquilino de la Casa Blanca poco después de su nombramiento, enteramente dedicado al proceso de Transformación (BUSH, George W: *A Blueprint for New Beginnings*, U.S. Government Printing Office, Washington D.C., 2001), o el artículo firmado por su secretario de Defensa (RUMSFELD, Donald H: «Transforming the Military», *Foreign Affaire*, volumen. 81, número 3, pp. 20-32, mayo-junio de 2002.

occidentales que todavía debatían sobre las características y efectos de la RMA; pronto la *transformación* sustituyó a la RMA como pilar del pensamiento estratégico occidental y eje de los procesos de planeamiento de la defensa de los países de nuestro entorno. Y es que los trágicos sucesos de verano de 2001 terminaron repentinamente con la pausa estratégica iniciada tras la caída del Telón de Acero, revelaron como el yihadismo –que había permanecido durmiente tras la política de bloques y se había configurado durante la década anterior²⁴– se había convertido en una seria amenaza para la seguridad internacional y mostraron al mundo que las acciones terroristas indiscriminadas eran, sin duda alguna, actos de guerra sin restricciones. Estos sucesos pusieron de manifiesto la extrema urgencia de adaptar las arquitecturas de seguridad y defensa de las naciones avanzadas –todavía grandes, rígidas y burocratizadas estructuras diseñadas para combatir en un conflicto convencional o nuclear contra el Pacto de Varsovia– a la realidad del siglo XXI; emplazaron la *transformación* en la cúspide del análisis estratégico global y en el foco del planeamiento de la defensa de Occidente; y las campañas afgana e iraquí permitieron poner a prueba la revolución²⁵.

Inicialmente, las espectaculares victorias cosechadas por las fuerzas de la coalición –y muy especialmente las estadounidenses– durante la invasión de Afganistán e Irak asombraron al mundo porque el potencial militar de Occidente parecía no tener límites. Al corroborar la validez del nuevo modelo militar fruto de la RMA, estos éxitos incrementaron la euforia revolucionaria y persuadieron a todos los países avanzados a avanzar en este modelo de *transformación*²⁶.

Y es que los resultados preliminares de las campañas no podían ser más sorprendentes: mientras en Afganistán una pequeñísima y heterogénea fuerza constituida *ad-hoc* para la misión, apoyada permanentemente desde el aire, equipada con revolucionarias tecnologías y usando avanzadas tácticas logró entrar triunfante en Kabul en poco más de un mes²⁷; en Irak fue una fuerza conjunta terrestre y anfibia con pleno apoyo aéreo la que luchó con un empuje y dinamismo nunca vistos hasta la fecha, paralizando el régimen iraquí, causando una total confusión entre las filas de su ejército,

²⁴ ANÓNIMO: *Imperial Hubris: How the West is Losing the War on Terror*, Brassey's, Washington D.C., 2004.

²⁵ KAGAN, Frederick: *Finding the target... opus citada*, pp. 293-340.

²⁶ BARDAJÍ, Rafael L.: «Las dos guerras de Donald Rumsfeld», *Política Exterior*, volumen 16, número 1, pp. 159-168, septiembre de 2002.

²⁷ BIDDLE, Stephen: *Afghanistan and the Future of Warfare: Implications for Army and Defense Policy*, U.S. Army Strategic Studies Institute, Carlisle Barracks, 2004.

anulando cualquier oposición militar digna de mención y logrando un triunfo fulminante, aplastante y decisivo en cuestión de semanas²⁸.

Sin embargo, entre las razones de estos éxitos se hallaban las semillas de los posteriores fracasos, puesto que con el paso de las operaciones de combate a las labores de estabilización, factores como el reducido volumen de fuerzas sobre el terreno y su imposibilidad para ejercer un control efectivo del territorio, el equipamiento empleado en ambas operaciones, su deficitaria preparación en tareas de seguridad, estabilización, apoyo militar a la reconstrucción o antiterrorismo, la inexistente inteligencia humana de la que disponían y el férreo control de las operaciones desde unos estados mayores situados a miles de kilómetros del teatro de operaciones; unidos éstos a la inexistencia de un plan coherente para su pacificación y las erróneas decisiones político-estratégicas que se tomaron al finalizar las operaciones de combate, facilitaron que en ambos escenarios estallara una insurgencia que ha permanecido activa hasta hoy en día a pesar de los esfuerzos de la comunidad internacional para acabar con ella.

El estallido de la insurgencia en Afganistán e Irak cogió desprevenida al grueso de la comunidad estratégica mundial puesto que pocos comprendían como una simple «guerra de guerrillas» podía poner en jaque a los poderosos ejércitos de Occidente²⁹. Y es que fascinados por el espejismo tecnológico, éstos parecían haber obviado algunos de los fundamentos de la guerra, en particular que ésta es siempre un choque de voluntades, que cualquier actor lucha con los medios que tiene a su alcance y que emplea las estrategias que más beneficios de pueden aportar³⁰. Así, frente a la supremacía militar de los invasores, el contendiente más débil se vio obligado a adaptarse y plantear respuestas que anularan o mitigaran tal superioridad y explotaran las vulnerabilidades políticas, sociales, jurídicas, morales, económicas o militares de estos ejércitos imposibles de batir en el terreno convencional³¹.

El auge de la insurgencia no sólo puso de manifiesto las limitaciones de la RMA en escenarios de baja o media intensidad; sino también las vastas dificultades políticas,

²⁸ DONNELLY, Thomas: *Operation Iraqi Freedom: a Strategic Assessment*, American Enterprise Institute Press, Washington D.C., 2004.

²⁹ La guerra irregular ha sido una constante a lo largo de la Historia desde la Antigüedad clásica. En este sentido, y a modo de ejemplo, no hace falta que nos movamos de nuestro país para contemplar un claro ejemplo de guerra irregular librada hace más de dos mil años: la larga y dura campaña romana contra las tribus celtíberas y lusitanas para hacerse con el control de la península Ibérica. Más ejemplos históricos pueden hallarse en BRAUD, Jacques: *La guerre asymétrique ou la défaite du vainqueur*, Éditions La Rocher, Mónaco, 2003.

³⁰ McIVOR, Anthony D. (ed.): *Rethinking the Principles of War*, U.S. Naval Institute Press, Annapolis, 2007.

³¹ Entre las numerosas vulnerabilidades de las sociedades occidentales puede citarse la volubilidad de la opinión pública doméstica y presión de la comunidad internacional; el pánico a las bajas propias y el temor a los daños colaterales; el sometimiento a unos usos y costumbres de la guerra restrictivos y anacrónicos; la ansiedad por los costes políticos y efectos electorales de las

estratégicas y operativas que entraña la estabilización de zonas hostiles, los monumentales costes humanos, materiales y políticos que conllevan las campañas de cambio de régimen y construcción nacional, o las nuevas y apremiantes necesidades operativas motivadas por la participación de los ejércitos occidentales en ambos conflictos. Este conjunto de elementos provocaron la desaparición definitiva de la RMA y comportaron un cambio de rumbo en el proceso de *transformación* militar.

Las primeras acciones que tomaron las potencias occidentales –encabezadas por Estados Unidos y posteriormente armonizadas por la Alianza Atlántica– fue primar la generación de aquellas capacidades militares más necesarias para satisfacer los requerimientos operativos presentes en detrimento del desarrollo de capacidades para los conflictos futuros. Para ello, rescataron los conceptos de «guerra irregular» (contraria a los usos y costumbres de la guerra)³² y «guerra asimétrica» (orientada a explotar las vulnerabilidades de las fuerzas regulares) a la vez que empezaron a releer los clásicos de la contrainsurgencia con el objeto de plantear una nueva estrategia coherente para acabar con la violencia insurgente que asolaba Afganistán e Irak y poder continuar con el proceso de construcción nacional de ambos países. Y para tal fin, procedieron a desarrollar las capacidades militares necesarias para combatir la amenaza irregular o asimétrica, conducir operaciones de contrainsurgencia y realizar labores de estabilización, seguridad, control del territorio o apoyo a los actores civiles en el marco de un enfoque integral a la gestión de crisis.

Y mientras Occidente estaba estudiando la amenaza irregular y revisando los pilares de la contrainsurgencia, Israel se enfrentaba a otra manifestación de guerra asimétrica más compleja, trascendente y potencialmente peligrosa que las anteriores y que articularía el análisis estratégico occidental durante los últimos años de este periodo histórico: el conflicto híbrido.

Originalmente definido en el año 2002 para advertir de las tácticas empleadas por la insurgencia chechena contra el Ejército ruso³³, el conflicto híbrido alcanzó fama mundial tras la guerra de verano de 2006 entre Israel y *Hezbollah*³⁴ y la posterior publicación del

operaciones; la exigencia de limitar su alcance, impacto y duración; la necesidad de emplear la fuerza de manera limitada y restrictiva o la incapacidad de implementar estrategias integrales a largo plazo.

³² Aunque los términos de «fuerza regular» y «fuerza irregular» son conceptos de uso común en el Derecho Internacional Humanitario, la definición más detallada de guerra irregular es: «A violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will.» (Department of Defense: *Irregular Warfare Joint Operating Concept*, p. 6, U.S. Government Printing Office, Washington D.C., 2007.

³³ NEMETH, William J.: *Future War and Chechnya: a Case for Hybrid Warfare*, Naval Postgraduate School, Monterrey, 2002.

³⁴ La operación *Recompensa Justa*, nombre que recibe la campaña militar israelí iniciada en julio de 2006 con objeto de liberar a los soldados hebreos capturados por las milicias de *Hezbollah*, terminar con los ataques de cohetes a las ciudades israelíes e

ensayo: *El conflicto en el siglo XXI: el advenimiento de la guerra híbrida*³⁵. En la actualidad, y junto con la guerra irregular, la amenaza híbrida constituye uno de los ejes que articulan el análisis estratégico internacional y uno de los principios que están guiando los procesos de *transformación* militar estadounidense y aliado.

Concebida como una forma de lucha posibilitada por la Era de la Información y fundamentada en las posibilidades que brinda la globalización y el libre acceso a las tecnologías avanzadas, la amenaza híbrida se caracteriza por la plena integración en tiempo y espacio de procedimientos típicamente convencionales con tácticas propias de la guerra irregular (desde acciones de propaganda, agitación e insurgencia hasta actividades de guerra informativa, guerra legal o ciberguerra), mezcladas éstas últimas con actos terroristas y conexiones con el crimen organizado para la obtención de fondos y la provisión de apoyos³⁶. La guerra híbrida entraña también el empleo de tecnologías avanzadas (sistemas no-tripulados, proyectiles guiados o sistemas de posicionamiento global)³⁷; la eficaz explotación de la dimensión propagandística e informativa para difundir su mensaje político y erosionar las opiniones públicas de sus oponentes; presenta una organización más sólida, cohesionada y con mayores ambiciones políticas que los grupos insurgentes tradicionales; una distribución interna flexible, adaptable y articulada en red³⁸; opera en un escenario marcado por su indefinición normativa y total desprecio a los usos y costumbres de la guerra y no duda en emplear todos los medios que estén a su disposición para infligir el máximo daño a su adversario.

Como puede observarse, con independencia de la originalidad y valor analítico de este concepto, la utilidad de la guerra híbrida no sólo reside en exponer la complejidad de los conflictos actuales y la creciente difuminación de la frontera entre lo regular y lo irregular; sino también por ilustrar a nuestras elites militares y políticas sobre la necesidad de superar el paradigma militar de la guerra fría y favorecer un proceso de Transformación que dote a las fuerzas armadas de las capacidades requeridas para que éstas puedan

implementar la resolución 1559 (2004) del Consejo de Seguridad de Naciones Unidas para desarmar y dismantelar las milicias chiítas del sur del Líbano, arrancó como una operación limitada pero escaló hacia una guerra abierta en la que Israel sufrió un duro revés a manos de *Hezbollah*: la sucesión de errores políticos y militares precipitaron una campaña improvisada y costosa que no logró conquistar los objetivos militares y puso en entredicho la supuesta invencibilidad de las todopoderosas Fuerzas de Defensa Israelíes, (CORDESMAN, Anthony D.: *Lessons of the 2006 Israeli-Hezbollah War*, Center for Strategic and International Studies, Washington D.C., 2007.

³⁵ HOFFMAN, Frank G.: *Conflict in the 21st Century: the Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, 2007.

³⁶ MATTIS, James N. y HOFFMAN, Frank G.: «Future Warfare: The Rise of Hybrid Warfare», *U.S. Naval Institute Proceedings* volumen 132, número 11, pp. 30-32, noviembre de 2005.

³⁷ GLENN, Russell W.: «Thoughts on Hybrid Conflict», *Small Wars Journal*, volumen 5, número 3, s/n, marzo de 2009.

³⁸ KILCULLEN, David: *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, Oxford University Press, Nueva York, 2009.

enfrentarse a cualquier adversario, en cualquier entorno operativo y en toda la gama de las operaciones.

En resumen, el 11 de septiembre de 2001 terminó con la aparente paz que estaba viviendo el mundo tras la caída del Telón de Acero y liquidó el modelo de seguridad y defensa vigente hasta entonces. Estos sucesos convirtieron la *transformación* en un imperativo estratégico y en la base del planeamiento de la defensa occidental en detrimento de la RMA, que fue relegada a un segundo plano. Sin embargo, el canto del cisne de esta revolución se produciría poco después, cuando las espectaculares victorias logradas por la coalición liderada por Estados Unidos en la invasión de Afganistán e Irak mostraron al mundo las enormes cualidades de este estilo de lucha que prometía triunfos rápidos y decisivos en toda la gama de operaciones mediante el empleo de una fuerza abrumadora. No obstante, el paso de las acciones de combate a las labores de estabilización y reconstrucción junto con el estallido de la insurgencia reveló sus limitaciones en escenarios de baja o media intensidad y permitió vislumbrar el cambiante rostro de la guerra.

Este baño de realismo evidenció las carencias de unos ejércitos todavía anclados en el paradigma de la guerra fría, mostró algunas de las nuevas amenazas que se cernían sobre la fuerza conjunta y expuso las limitaciones de una *transformación* excesivamente tecnocéntrica y centrada en la lucha convencional. Tales factores acabaron definitivamente con el furor revolucionario de la década anterior, desterraron la RMA del análisis estratégico y del planeamiento de la defensa occidental y motivaron un cambio de rumbo en la *transformación* con el fin de generar las capacidades militares necesarias para resolver los problemas operativos presentes.

Este giro estratégico provocó que el planeamiento de la defensa occidental pasara a articularse en torno a la generación de capacidades militares para la estabilización posconflicto, la construcción nacional o la lucha contra la insurgencia; y el pensamiento estratégico primara el estudio de las amenazas irregulares e híbridas, consideradas por muchos como el mayor peligro que se cernía sobre los ejércitos avanzados. No obstante, el renovado interés político, militar y académico por la guerra asimétrica, el conflicto de baja intensidad o el planeamiento de la defensa de contingencia, relegaron a un lugar secundario otros riesgos más *tradicionales* que estaban surgiendo durante este mismo periodo y que no serían integrados en el pensamiento estratégico de Occidente hasta fechas recientes: el peligro de un Pakistán fallido, el arma atómica norcoreana, la

proliferación nuclear persa, la capacidad antisatélite china, la ciberguerra sobre Estonia o la guerra convencional con tintes posmodernos entre Rusia y Georgia.

El arte de la estrategia en un mundo incierto

El último hito de nuestra historia reciente se sitúa el 15 de septiembre de 2008, cuando la quiebra del banco de inversión Lehman Brothers reveló la fragilidad del sistema financiero global y las debilidades estructurales de Occidente, e inauguró una nueva etapa histórica marcada por la frugalidad económica, el control del gasto y la escasez de recursos. En el campo de la defensa, mientras la crisis económica ha provocado la contracción del gasto militar de los países avanzados y las largas campañas imperiales han revelado los costes políticos, económicos, humanos o materiales de la guerra y la ilusión de las operaciones de construcción nacional; la *transformación* se ha reafirmado como el pilar del planeamiento de la defensa occidental y el análisis estratégico ha identificado nuevos riesgos, ha codificado nuevas amenazas y ha constatado nuevas áreas de potencial conflicto.

En primer lugar: la crisis económica mundial ha provocado una importante contracción del presupuesto público de los países occidentales. Aunque esta disminución se está observando en todas las esferas de actuación del Estado, donde más está incidiendo es en el ámbito de la seguridad y la defensa, puesto que estas políticas públicas no responden a ninguna demanda social concreta, no proporcionan resultados tangibles, sus efectos sobre los electorados son muy limitados y hoy en día la sensación de amenaza que resurgió en el año 2001 parece haberse debilitado. Esta contracción del gasto militar no sólo está obligando a revisar a la baja los objetivos de fuerzas, catálogos de capacidades y los planes de modernización de los ejércitos occidentales; sino también está dificultando su planeamiento de la defensa puesto que cualquier decisión que se tome hoy determinará el desarrollo de los ejércitos futuros.

Y es que en una etapa marcada por la reformulación de la *transformación* militar, las limitaciones presupuestarias, la incertidumbre estratégica, la aceleración tecnológica y el incremento de las labores a realizar por los ejércitos, son muchos los países que deben plantear hoy las capacidades militares que necesitarán para las guerras del mañana, sin olvidar que cualquier opción que tomen ahora determinará el modelo de fuerzas armadas futuras y su habilidad para afrontar con éxito los retos emergentes³⁹. En consecuencia, las potencias occidentales deberán elegir qué capacidades militares desarrollar, cuáles

³⁹ Para conocer los ejes sobre los que se articula el debate, GRAY, Colin S.: *Transformation and Strategic Surprise*, U.S. Army Strategic Studies Institute, Carlisle Barracks, 2005.

descartar y cuáles conservar; y para ello deberán establecer unos niveles de ambición realistas y asequibles, promover unos análisis estratégicos serios y cautos, superar la falsa dicotomía entre fuerzas específicas para conflictos convencionales o irregulares y vencer las inercias de unas instituciones militares reticentes al cambio. De realizarse, estas medidas comportarán profundas transformaciones en la concepción, administración, funcionamiento y gestión de la defensa, y sus efectos serán especialmente visibles en el continente europeo, puesto que sus disfuncionales entramados de defensa y sus ejércitos todavía anclados en la guerra fría deberán ser completamente replanteados si se pretende que éstos continúen siendo relevantes para los conflictos futuros. Es por ello que la *transformación* de la defensa y la institucionalización del cambio entre las Fuerzas Armadas en una coyuntura de indefinición estratégica y escasez de recursos se plantean como los mayores retos que tienen por delante los entramados de seguridad y defensa occidentales.

Igualmente, se ha puesto de manifiesto la incapacidad que presentan las democracias avanzadas para mantener largas campañas militares en el contexto de «guerras de elección» como los Balcanes o Libia y «guerras de necesidad» como Afganistán e Irak⁴⁰. Después de observar la evolución de los conflictos recientes, Occidente ha constatado la inviabilidad práctica de las labores de construcción nacional y las dificultades de las operaciones de cambio de régimen; la exigencia de definir una situación final deseada realista, asequible, asumible y vinculada a una estrategia de salida; la volubilidad de la opinión pública y el poder de los medios de comunicación de masas, el frágil apoyo popular a todas aquellas intervenciones que no se presenten como humanitarias, sin solución aparente o que se dilaten en el tiempo; la carencia de herramientas específicas para la estabilización posconflicto; la dificultad de los ejércitos modernos para mantener largos despliegues, adaptarse a un entorno en constante evolución, operar en toda la gama de operaciones o regenerar la fuerza después de casi 10 años de conflicto. Pero sobretodo, el inicio de esta etapa ha servido para que Occidente observe la inmutable naturaleza de la guerra, en la que el horror, la destrucción y la muerte son sus elementos definidores; y debería comprender que la fuerza armada debe emplearse como último recurso, de manera racional y siempre orientada a la consecución de unos objetivos claramente definidos, realistas y alcanzables en tiempo y espacio.

En tercer lugar: la progresiva disminución del interés de la comunidad de defensa occidental por las campañas afgana e iraquí ha coincidido con una renovada atención por

⁴⁰ FOLEY, Conor: *The Thin Blue Line: How Humanitarianism Went to War*, Verso, Nueva York, 2008.

la configuración de los «nuevos» riesgos y amenazas a la seguridad global. Así, las grandes contingencias de la pasada década –aunque limitadas e incapaces de alterar la estructura del sistema internacional– como la larga guerra contra el terror, la construcción de Estados, la insurgencia o la guerra irregular e híbrida; parecen haber dejado paso a otros peligros susceptibles de perturbar el equilibrio estratégico global como la proliferación de armamento de destrucción masiva, la inestabilidad del mundo árabe y musulmán, la competición entre los poderes emergentes y las potencias consolidadas por la hegemonía regional y el control de los recursos o las amenazas que se ciernen sobre el libre acceso a los bienes comunes globales como los mares, el cielo, el espacio y el ciberespacio⁴¹.

La inclusión de estos riesgos y amenazas de distinta naturaleza, procedencia y alcance en la agenda estratégica occidental ha supuesto un importante baño de realismo que no sólo ha motivado el resurgimiento del análisis geopolítico y el retorno al pragmatismo político-estratégico⁴²; sino también ha recordado a las potencias occidentales que si pretenden continuar siendo relevantes en los asuntos globales, no sólo deberán prepararse para luchar en toda la gama de las operaciones, sino sobre todo garantizar su supremacía militar convencional frente a cualquier adversario avanzado. Y para ello, no será suficiente sólo con dominar las operaciones terrestres, navales y aéreas, sino también la esfera informativa, cibernética y espacial. Estas tres dimensiones que escapan al control de los estados y pueden emplearse tanto de forma autónoma como para multiplicar el poder terrestre, naval y aéreo en una amplia variedad de acciones ofensivas y defensivas, lograrán su pleno potencial militar cuando los ejércitos sigan los pasos iniciados por China, Rusia y Estados Unidos e institucionalicen completamente estos nuevos dominios e implementen las capacidades necesarias para operar en el espacio, el ciberespacio y en la esfera de la información⁴³.

En conclusión, aunque todavía es pronto para establecer los contornos de esta etapa histórica, y con el conocimiento que el futuro nunca se amoldará a nuestras expectativas, son muchos los indicios que sugieren que ésta se caracterizará por la consolidación de los poderes emergentes, el estancamiento global estadounidense y la demostración definitiva de la irrelevancia estratégica europea. En el campo de la seguridad podremos observar como la proliferación de una amplia gama de riesgos y amenazas de distinta

⁴¹ DENMARK, Abraham M. *et al.*: *Contested Commons: the Future of American Military Power in a Multipolar World*, Center for a New American Security, Washington D.C., 2010.

⁴² FOJÓN, Enrique: «El análisis estratégico: la vuelta al pragmatismo», *Documento de Trabajo* 15/2009, Real Instituto Elcano, Madrid, 2009.

⁴³ ARQUILLA, John y RONFELDT, David (eds.): *In Athena's Camp... opus citada*, pp. 23-60 y 217-274.

naturaleza, procedencia e impacto no sólo perturbará el frágil equilibrio del presente orden global y pondrá a prueba la cohesión de la comunidad internacional y la eficacia de las organizaciones de seguridad; sino que también revelará las enormes debilidades de nuestras sociedades occidentales.

Finalmente, en la esfera militar veremos como la diversidad de potenciales adversarios, los múltiples métodos y medios de combate disponibles y los variados escenarios de confrontación posibles provocarán que las Fuerzas Armadas deban prepararse para realizar una amplia gama de labores, desarrollar nuevas competencias y superar viejos paradigmas para garantizar su continua adaptación a un escenario táctico, operacional y estratégico en permanente evolución. La superación de estos desafíos exigirá a Occidente determinación política, respuestas imaginativas y un pensamiento estratégico pragmático y realista, puesto que solamente así podrá navegar con garantías en las turbulentas aguas del mundo del siglo XXI.

GUILLEM COLOM PIELLA
Doctor en Seguridad Internacional

CIBERESPACIO: LA NUEVA DIMENSIÓN DEL ENTORNO OPERATIVO

Introducción

La rápida evolución de las Tecnologías de la Información y de las Comunicaciones (TIC) está aumentando la velocidad, capacidad, agilidad, eficiencia y utilidad de las redes y sistemas actuales, tanto en el ámbito civil como militar. Estas tecnologías están cambiando el modo en el que las personas interactúan entre sí y también con su entorno.

Análogamente, las Fuerzas Armadas no sólo dependen de las TIC y de los sistemas de información para comunicarse, mandar y controlar las operaciones, coordinar acciones de fuego, obtener y distribuir información de inteligencia, realizar acciones de vigilancia y reconocimiento, entre otras actividades militares, sino que, además, están transformando el modo en el que éstas se planifican y ejecutan. Al mismo tiempo, los adversarios, en cualquiera de sus formas (naciones, grupos criminales o terroristas, facciones extremistas, etc.) tienen acceso y pueden utilizar las mismas tecnologías de un modo completamente innovador y singular.

Dado que las Fuerzas Armadas son, cada vez más, dependientes de los recursos electromagnéticos y las redes informáticas, los cuales están en un continuo proceso de convergencia, está emergiendo un «campo de batalla cibernético y electromagnético». Como la tecnología que permite la comunicación y procesamiento de la información cambia tan rápidamente, las Fuerzas Armadas deben evaluar continuamente qué aptitudes y capacidades son las necesarias para conseguir, conservar y explotar las ventajas en este emergente campo de batalla.

El modo en el que las tecnologías del ciberespacio se integran y emplean, según las circunstancias operativas de cada momento, afectará significativamente al desarrollo y resultado de las operaciones militares. Si bien es importante estar a la vanguardia en el conocimiento y aplicación de las TIC, no lo es menos el establecer una aproximación

integral a todos los aspectos de las ciberoperaciones y ser capaces de obtener ventaja al combinarlos y adaptarlos a las condiciones operativas de cada momento. Como en el resto de las dimensiones del entorno operativo (tierra, mar, aire y espacio exterior), conseguir el dominio en el ciberespacio implica progresar simultáneamente en dos aspectos de las operaciones: obtener superioridad y mantenerla.

Aunque el empleo de las tecnologías emergentes antes de que lo hagan los adversarios proporciona una gran ventaja, deben tenerse en cuenta, y mitigarse, las vulnerabilidades y dependencias que genera su implementación en las redes, sistemas y sensores propios. Probablemente, será incluso más importante conseguir la desactivación, interrupción y anulación de las mismas capacidades en poder de los adversarios. Para ello, las Fuerzas Armadas deben integrar capacidades desde un principio, convirtiéndolas en los elementos de una misma dimensión de las operaciones modernas. Tal integración conducirá a la sinergia, el progreso rápido y la consecución de un alto número de objetivos. Sin embargo, sino se consigue dicha integración el progreso de las operaciones será desigual, en el mejor de los casos, o se producirán fracasos operativos.

Conseguir la supremacía en el ciberespacio requiere conocimientos avanzados en teoría de la información, electrónica, propagación de ondas radioeléctricas, entre otros, así como en la aplicación de éstos a las tácticas, operaciones y estrategias militares. Aunar estos conocimientos con la práctica militar moderna es fundamental para obtener «conciencia de la situación» (*situational awareness*) de las ciberoperaciones y, por tanto, contribuir a la consecución de los objetivos del mando. Igual de crítico es transformar la actual aproximación fragmentada a esta dimensión de las operaciones en otra que sea sistemáticamente integral.

Aunque es factible alcanzar objetivos militares solo mediante el empleo de las ciberoperaciones, éstas no son generalmente un fin en sí mismas sino parte integral de cualquier tipo de operación. Las ciber-operaciones deben estar dirigidas a obtener la superioridad en el ciberespacio mediante la integración de las dos líneas de acción mencionadas más arriba: obtener ventaja y conservarla. El mando conducirá ciberoperaciones para conservar la libertad de acción en la dimensión del campo de batalla que constituyen el ciberespacio y el espectro electromagnético y, al mismo tiempo, negar tal libertad al enemigo en el momento y espacio oportunos para permitir diferentes acciones operativas en las otras dimensiones del campo de batalla.

Las Fuerzas Armadas españolas, tanto en el ámbito específico de los Ejércitos y la Armada, como en el conjunto, liderado por el Estado Mayor de la Defensa, desarrollan distintos Programa de Información y Comunicación (CIS) con el objetivo de proporcionar redes y sistemas que incorporen las tecnologías precisas para proporcionar los servicios y aplicaciones que apoyen a los mandos militares en el cumplimiento de sus misiones. Por tanto, las Fuerzas Armadas están creando y mejorando su propia parte del «ciberespacio global» para obtener la mayor ventaja o ser lo más competitivos posible en la dimensión cibernética y electromagnética del campo de batalla pero, al mismo tiempo, generando nuevas dependencias y vulnerabilidades en las capacidades militares.

Una aproximación al concepto de ciberespacio

Antes de abordar las capacidades y componentes de las ciberoperaciones es conveniente realizar una breve aproximación al concepto de ciberespacio.

El ciberespacio es el conjunto de medios y procedimientos basados en las TIC y configurados para la prestación de servicios.

El ciberespacio está constituido por *hardware*, *software*, Internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socioeconómica de cualquier nación, y en especial aquellos ligados a sus infraestructuras críticas, figura 1.

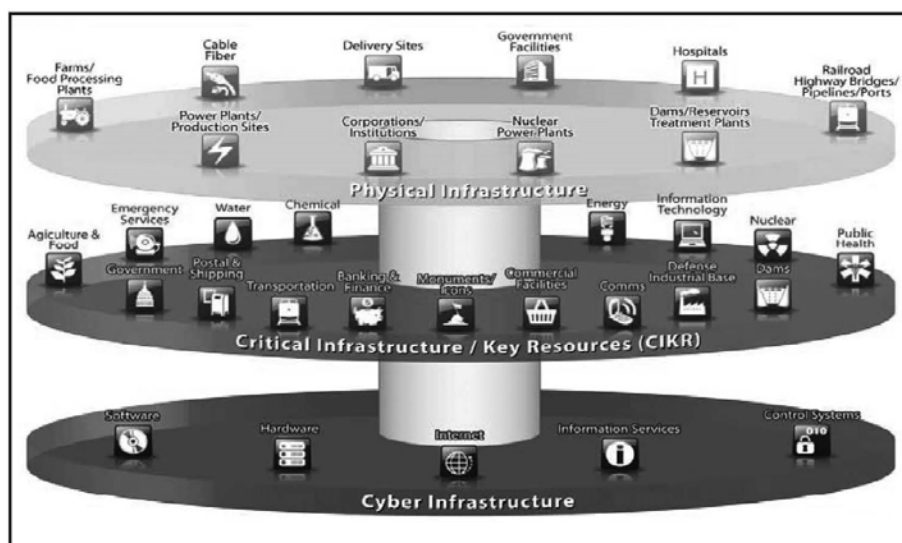


Figura 1.— Ciberespacio.

El ciberespacio se vertebra sobre tres capas superpuestas: capa física, capa lógica y capa social. Además, en cada capa existen componentes en concreto, cinco componentes distribuidos en las tres capas, figura 2: componente geográfica, componente de las redes físicas, componente de las redes lógicas, persona y ciberidentidades.

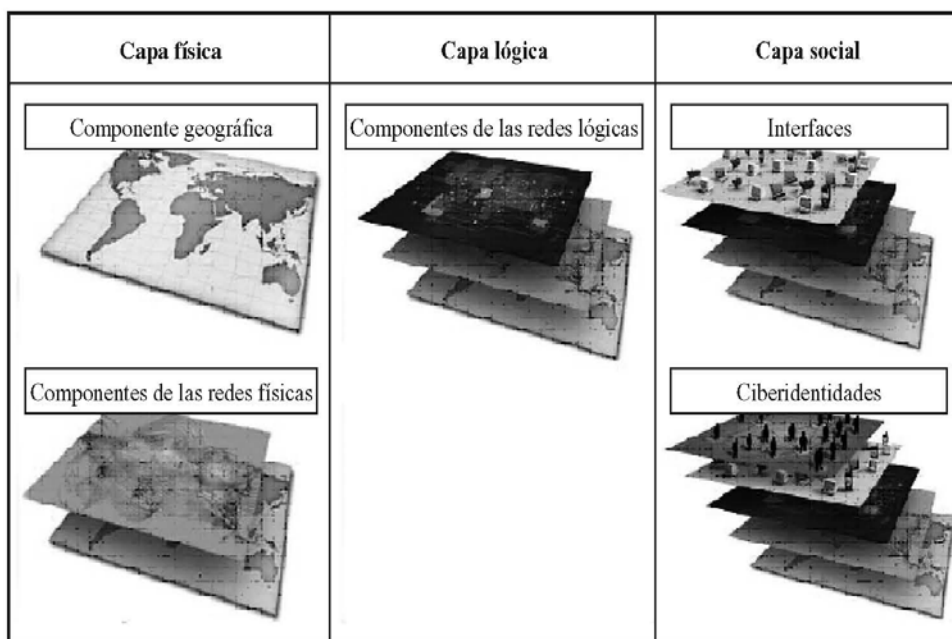


Figura 2.— Capas del ciberespacio.

La *capa física* engloba la «componente geográfica» y la «componente de las redes físicas». La componente geográfica se refiere a la localización física de los elementos de la componente de las redes físicas. La componente de las redes físicas está formado por el hardware e infraestructura que soportan las redes y sus conectores físicos (cableado, cifradores, routers, servidores, ordenadores, etc.).

La *capa lógica* está formada por la componente de redes lógicas que son las conexiones lógicas que existen entre los nodos de las redes, entendiendo por nodo cualquier dispositivo que está conectado a las redes CIS.

La *capa social* está formada por los componentes persona y ciber-identidad. El componente persona está formado por los individuos que interactúan con el ciberespacio. La relación entre personas y ciberidentidades puede ser de 1 a n y de n a 1, es decir, una persona puede disponer de una o más ciberidentidades y una ciberidentidad puede ser utilizada por una o más personas. Estas ciberidentidades pueden ser reales o

suplantadas, lo que permite gozar de cierto anonimato o impunidad en las acciones que se ejecuten en el ciberespacio siendo, por tanto, difícil relacionar de manera unívoca una ciberidentidad con una persona. Las ciber-identidades están constituidas, entre otros, por cuentas de correo electrónico, cuentas de usuarios en redes o perfiles en redes sociales.

Cíberoperaciones: componentes y capacidades

Denominamos ciberoperaciones al empleo de capacidades cibernéticas cuyo propósito es la consecución de objetivos militares en, o a través de, el ciberespacio. Las ciberoperaciones no son un fin en sí mismas, sino que forman parte integral de cualquier tipo de operación militar y su concepto surge de manera inmediata al considerar el ciberespacio una dimensión más del entorno operativo a teatro de operaciones. Así, a las dimensiones clásicas: tierra, mar, aire y espacio, se suma esta quinta dimensión, el ciberespacio.

Las acciones que comprenden las ciber-operaciones pueden ser agrupadas en cuatro elementos, a saber:

1. Ciberoperaciones de red.
2. Cibercombate.
3. Ciberapoyo.
4. Conocimiento de la cbersituación.

A continuación se describirán las acciones y funciones de cada uno de estos cuatro elementos, así como las capacidades requeridas para poder conducir tales acciones y ejecutar las funciones.

La figura 3 esquematiza la interrelación entre los cuatro elementos de las ciberoperaciones.

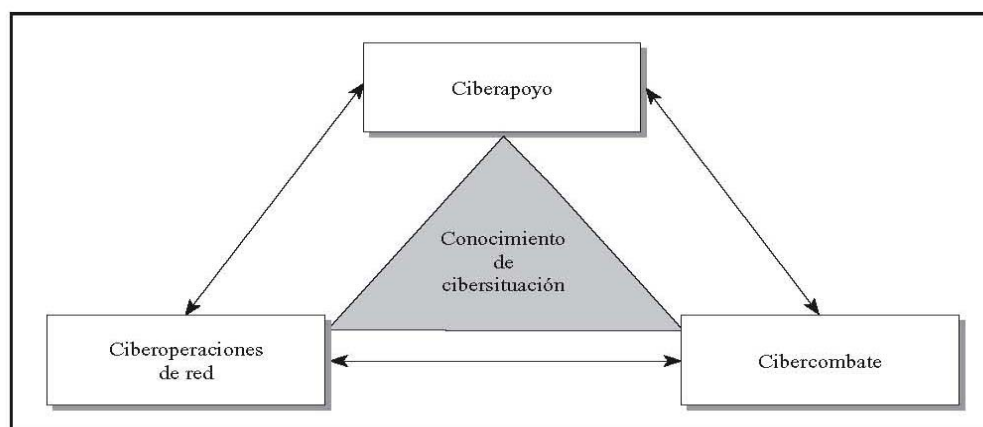


Figura 3.— *Interrelación entre los cuatro elementos de las ciberoperaciones.*

CÍRBEOPERACIONES DE RED

DESCRIPCIÓN

Este componente de las ciberoperaciones es el que permite el establecimiento, operación, mantenimiento, defensa, mando y control de las redes y sistemas militares, así como de las infraestructuras y recursos críticos.

Este componente consiste en tres elementos básicos:

1. *Gestión corporativa*: conjunto necesario de tecnologías, procesos y normativas para operar eficazmente las redes y sistemas del ciberespacio propio.
2. *Gestión de contenidos*: conjunto de tecnologías, procesos y normativa para proporcionar el conocimiento de la información relevante, el acceso automático a información recurrente o recientemente descubierta, así como el suministro de información en tiempo útil, de modo eficiente y seguro, y en un formato adecuado.
3. *Ciberdefensa*: conjunto de acciones que combinan el análisis y gestión de riesgos, la defensa de las redes y sistemas, la protección de las infraestructuras críticas, de modo que se prevenga, detecte y, en último caso, responda a la capacidad de un adversario de privar o manipular la información y/o la infraestructura que la respalda. La ciberdefensa ha de estar integrada con los aspectos dinámicos y defensivos del componente *cibercombate* para proporcionar una defensa en profundidad.

La naturaleza rápidamente cambiante del ciberespacio exige a las unidades tácticas y operacionales disponer de, o a tener acceso a, las capacidades y conocimientos expertos para proteger sus redes y sistemas, detectar y prevenir, en tiempo real, ataques sobre los mismos y tener la posibilidad de responder a dichos ataques.

La disponibilidad de información y productos de inteligencia a través de las redes y sistemas militares es crítica para la conducción de todas las operaciones y el éxito global de las misiones. Los mecanismos y componentes de defensa y redundancia de los sistemas y redes críticos deben ser suficientemente robustos para proporcionarles seguridad (integridad, confidencialidad y disponibilidad), incluso a pesar de los esfuerzos del adversario por atacarlos o explotar sus vulnerabilidades. Hay que asumir que los adversarios potenciales poseen una capacidad significativa para realizar ciberoperaciones, por lo que las Fuerzas Armadas deberán ser capaces de combatir empleando las redes y sistemas en un estado degradado, sobre todo en los escalones táctico y operacional, por lo que el adiestramiento de las unidades en tales condiciones degradadas es fundamental para asegurar la continuidad de las operaciones.

Las funciones más típicas del componente «ciberoperaciones de red» son:

- Planificar y diseñar (ingeniería).
- Instalar y operar las redes, sistemas y servicios.
- Mantener las redes, sistemas y servicios.
- Gestionar los contenidos.
- Proteger las redes, sistemas y servicios.
- Proporcionar datos para el propio conocimiento de la cbersituación.

CAPACIDADES

Para conducir eficazmente las ciberoperaciones de red, las unidades de las Fuerzas Armadas deben contar con una serie de capacidades, que se listan a continuación:

- Operar una capacidad corporativa¹ para redes de telecomunicaciones e informáticas que permitan manejar información clasificada hasta grado *Top Secret (Secreto)* a nivel Brigada y superior, y hasta *Secret (Reservado)* en niveles inferiores a Brigada. Deben incluirse niveles de clasificación de coaliciones y aliados.
- Proporcionar conectividad global a la red de comunicaciones corporativa para asegurar que las operaciones de red pueden realizarse extremo a extremo, y así dar apoyo a los mandos de combate críticos y proporcionarles libertad de acción.
- Proporcionar redes de comunicaciones corporativas que sean interoperables a nivel conjunto nacional y con organizaciones internacionales –Organización del Tratado del Atlántico Norte (OTAN), Organización de Naciones Unidas (ONU)– y organizaciones no gubernamentales (ONG) para asegurar que las operaciones de red pueden realizarse extremo a extremo, y así dar apoyo a los mandos de combate críticos y proporcionarles libertad de acción.
- Integrar las redes de aliados en emplazamientos en territorio nacional y en zona de operaciones, incluyendo la capacidad de integrarse en las redes de aliados con distintas necesidades de compartir información de inteligencia, de modo que las operaciones conjuntas y multinacionales sean eficaces y asegurar la libertad de acción.

¹ El término *corporativo* es empleado con el significado de global dentro de una determinada organización o corporación. Dicha organización puede ser cualquiera de los Ejércitos o Armada o todas las Fuerzas Armadas en su conjunto, si se pretende tener un sistema o red eficaz, seguro y correctamente gestionado.

- Definir las funciones, responsabilidades y autoridades de socios públicos y privados para asegurar los elementos comerciales de las redes y sistemas que son empleados por la Fuerzas Armadas y asegurar la libertad de acción.
- Proporcionar un sistema de mando y control para obtener, procesar y difundir información relativa a las operaciones de red que faciliten la toma de decisiones del mando y la eficacia de las operaciones.
- Proporcionar acceso autenticado de los usuarios a las capacidades de las ciberoperaciones para permitir una acción de mando distribuida, remota y móvil.
- Agregar todos los datos relativos a los recursos informáticos conectados a la red corporativa para proporcionar al mando apoyo de operaciones de red extremo a extremo y contribuir al propio conocimiento de la cibersituación.
- Monitorizar el estado de las redes y sistemas, realizar el mantenimiento preventivo y correctivo de los mismos, así como obtener estadísticas de uso de un modo completamente automático e instantáneo para así proporcionar al mando apoyo de operaciones de red extremo a extremo y contribuir al propio conocimiento de la cibersituación.
- Operar en condiciones degradadas de funcionamiento de redes y sistemas para asegurar la eficacia de la acción de mando y de las operaciones y asegurar la libertad de acción.
- Proporcionar defensa en profundidad en las redes y sistemas para proporcionar al mando apoyo de operaciones de red extremo a extremo.
- Proteger las redes y sistemas de ataques electrónicos, incluidos los ataques electromagnéticos, para proporcionar al mando apoyo de operaciones de red extremo a extremo y asegurar la libertad de acción.
- Detectar e informar, en tiempo real, de amenazas cibernéticas para contribuir a la seguridad en profundidad y al propio conocimiento de la cibersituación.
- Detectar y monitorizar, en tiempo real, las intrusiones de red y las actividades no autorizadas para contribuir a la defensa en profundidad, proporcionar apoyo de operaciones de red a los mandos, asegurar la libertad de acción y contribuir al propio conocimiento de la cibersituación.
- Analizar y comprender, en tiempo real, la naturaleza de las actividades maliciosas y no autorizadas que ocurren en las redes y sistemas para contribuir a la defensa en

profundidad, proporcionar apoyo de operaciones de red a los mandos, asegurar la libertad de acción y contribuir al propio conocimiento de la cbersituación.

- Atribuir acciones en redes propias y enemigas para dar apoyo a las acciones de operaciones de red y cibercombate.
- Proporcionar protección física y de ciberoperaciones contra ataques letales, y no letales, sobre infraestructuras críticas y otros recursos claves durante todas las fases de cualquier tipo de operación para contribuir a la defensa en profundidad, proporcionar apoyo de operaciones de red a los mandos, asegurar la libertad de acción.
- Conseguir el conocimiento, el acceso y la distribución de información para proporcionar apoyo «extremo a extremo» a las ciberoperaciones de red.
- Proporcionar capacidades para la ciberoperaciones a naciones aliadas para que contribuyan a la defensa en profundidad del ciberespacio aliado, así como posibilitar operaciones combinadas y conjuntas eficaces.
- Compartir información y colaborar con entidades públicas y privadas sobre todos los aspectos relacionados con la operación de redes y protección de infraestructuras críticas y otros recursos clave para contribuir a la defensa en profundidad y proporcionar apoyo de operaciones de red a los mandos.
- Asegurar la confidencialidad, integridad y disponibilidad de las capacidades esenciales de las ciberoperaciones para proporcionar apoyo de operaciones de red extremo a extremo a los mandos.
- Desarrollar una base geoespacial estándar para facilitar a todos los mandos información esencial, crear una base cartográfica común, así como mostrar y compartir esta información en un Cuadro Operativo Conjunto (COP).
- Crear, cambiar y distribuir órdenes (orales y escritas) para permitir las comunicaciones entre puestos de mando, plataformas y mandos gubernamentales.
- Proporcionar apoyo para el entrenamiento y adiestramiento para preparar las operaciones empleando herramientas informáticas que representen con precisión todo el espectro de misiones y condiciones operativas.

CÍBERCOMBATE

DESCRIPCIÓN

El cibercombate es el componente de las ciberoperaciones que emplea el ciberespacio para causar efectos más allá de las redes y Sistemas TIC que permitan detectar, disuadir

o derrotar a los adversarios. Las capacidades para el cibercombate tienen como objetivo las redes informáticas y de telecomunicaciones, así como los procesadores, sensores y controladores que se hallan en cualquier equipamiento, sistema, plataforma o infraestructura. El cibercombate emplea básicamente tres elementos o conjunto de acciones: ciberexplotación, ciberataque y ciberdefensa Dinámica, y lo debe hacer de un modo totalmente coordinado con las acciones incluidas en los componentes de ciberoperaciones de Red y ciberapoyo. A continuación se describen brevemente cada uno de estos elementos:

- *Ciberataque*: conjunto de acciones que combinan los ataques a redes informáticas con otros como ataques electrónicos², ataques físicos, etc., con el objetivo de manipular la información o denegar el acceso a la misma por parte del enemigo o la propia infraestructura.
- *Ciberexplotación*: conjunto de acciones que combinan la explotación de redes informáticas con otras tales como la Inteligencia de Señales (SIGINT) para obtener información de inteligencia.
- *Ciberdefensa dinámica*: conjunto de acciones que combinan normativa, inteligencia, sensores y procesos automatizados para identificar y analizar actividades maliciosas, encontrar correlaciones entre ellas y ejecutar acciones de respuesta preaprobadas para neutralizar ataques antes de que puedan causar daños. Este tipo de acciones debe usar principios defensivos de seguridad, defensa en profundidad y el empleo máximo de acciones ofensivas para confrontar las amenazas cibernéticas. Estas acciones incluyen las de vigilancia y reconocimiento para proporcionar a los mandos las alertas tempranas relativas a acciones previstas del enemigo. La ciberdefensa dinámica ha de ser integrada con los aspectos defensivos del componente operaciones de red.

Las funciones más típicas del componente cibercombate de las ciberoperaciones son:

- Recoger y analizar los datos de redes, sistemas y servicios.
- Estudiar y caracterizar las amenazas.
- Identificar, seguir y explotar las actividades enemigas.
- Suministrar datos para el propio conocimiento de la ciber situación.
- Conducir la ciberdefensa dinámica.

² Ataque electrónico: uso de la energía electromagnética para atacar a las personas, instalaciones o el equipamiento con el objetivo de degradar, neutralizar o destruir la capacidad de combate enemiga. Es considerado una forma de fuego.

- Ayudar en la investigación de ataques para determinar su origen.

CAPACIDADES

Para conducir acciones de cibercombate, las Fuerzas Armadas requieren, al menos, las capacidades que se enumeran a continuación:

- Acceder a redes, sistemas o nodos objetivo por medios directos o remotos para asegurar los accesos necesarios que permitan acciones de ciber-combate sobre objetivos transitorios.
- Permitir el acceso recurrente a redes, sistemas o nodos objetivo por medios directos o remotos para asegurar los accesos necesarios que permitan acciones de cibercombate sobre objetivos transitorios.
- Acceder a hardware y software del enemigo por medios directos o remotos para asegurar los accesos necesarios que permitan acciones de cibercombate y ciberapoyo.
- Acceder, recopilar y explotar la información del enemigo por medios directos o remotos para detectar, impedir, denegar y derrotar las acciones del enemigo y su libertad de acción.
- Permitir la capacidad de agregar, gestionar, descifrar, traducir (lingüísticamente), analizar e informar sobre todos los datos en sistemas de gestión del conocimiento para apoyar las ciberoperaciones y la acción de mando.
- Proporcionar capacidades remotas y expedicionarias de cibercombate para detectar, impedir, denegar y derrotar las acciones del enemigo y su libertad de acción.
- Atacar (denegar, degradar, perturbar y destruir) las redes e infraestructuras enemigas para detectar, impedir, denegar y derrotar las acciones del enemigo y su libertad de acción.
- Proporcionar capacidades de respuesta a intrusiones y ataques para detectar, impedir, denegar y derrotar las acciones del enemigo, integrar la defensa en profundidad con acciones de ciberoperaciones de red, asegurar la libertad de acción propia y denegar la del enemigo en los lugares y momentos apropiados.
- Atacar redes enemigas para detectar, impedir, denegar y derrotar las acciones y su libertad de acción.
- Atacar (denegar, degradar, perturbar y destruir) los procesadores y controladores del equipamiento enemigo y sus sistemas para detectar, impedir, denegar y derrotar sus acciones, integrar la defensa en profundidad con acciones de operaciones de red,

asegurar la libertad de acción propia y denegar la del enemigo en los lugares y momentos apropiados.

- Proporcionar conocimiento de estado de las redes enemigas y de cualquier otra de interés para contribuir al conocimiento de la situación del mando y permitir las ciberoperaciones y resto de operaciones militares.
- Conocer y comprender las arquitecturas físicas y lógicas de las redes enemigas, u otra cualquier de interés, para permitir todos los aspectos de las ciberoperaciones.
- Buscar, localizar y prever las actividades del enemigo en el ciberespacio para permitir las acciones de cibercombate, ciberoperaciones de red y Conocimiento de la cbersituación.
- Atacar la información del usuario para disuadirle, socavarle y engañarle, además de apoyar al mando en el cumplimiento de su misión.
- Mitigar o superar las medidas defensivas del enemigo para poder ejecutar acciones de cibercombate.
- Atacar las infraestructuras que sustentan el ciberespacio enemigo para apoyar las ciberoperaciones y la consecución de los objetivos del mando.

CIBERAPOYO

DESCRIPCIÓN

El ciberapoyo es un proceso continuo que tiene como objetivos:

- Responder, en tiempo y forma, a las necesidades cibernéticas del mando adaptándose a la continua maleabilidad del ciberespacio global, proporcionando herramientas cibernéticas, ofensivas y defensivas, que garanticen la defensa del ciberespacio global de las Fuerzas Armadas y permitan ejecutar ciberoperaciones.
- Proporcionar al mando nuevos servicios cibernéticos así como evolucionar los servicios ya existentes.
- Garantizar la seguridad del ciberespacio global que se encuentra a disposición de las Fuerzas Armadas minimizan los riesgos, respondiendo eficazmente a los ciberataques e intentando anticiparse a futuras acciones de ataque.

CAPACIDADES

Estos objetivos se alcanzaran siempre y cuando se ejecutan el siguiente conjunto de actividades:

- Ejecutar todos los aspectos de operación y mantenimiento adaptativo, perfectivo y preventivo de redes, sistemas y servicios relacionados con las ciberoperaciones.
- Ejecutar procesos de ingeniería inversa así como aquellos análisis técnicos necesarios para permitir acciones eficaces de cibercombate y ciberoperaciones de red.
- Realizar análisis legales y normativos para apoyar las acciones de cibercombate y los procesos de toma de decisión del mando.
- Realizar análisis de riesgos que permitan identificar las principales vulnerabilidades del ciberespacio global de las Fuerzas Armadas. Este análisis de riesgo debe circunscribirse dentro de un proceso sistemático y riguroso ejecutado con una metodología reconocida y herramientas adecuadas (ejemplo, la herramienta PILAR ha sido recientemente adoptada por la Agencia BICES como herramienta para el análisis de riesgos de sus sistemas). Un correcto y sistemático análisis de riesgos proporcionara una estado de situación «veraz» que cual redundara en una mejor defensa del ciberespacio global de las Fuerzas Armadas. Por el contrario, un análisis de riesgos incompleto constituye el primer eslabón de un ciberespacio vulnerable y potencialmente expuesto al adversario.
- Realizar pruebas de intrusión, como parte del análisis y gestión de riesgos, analizando las amenazas y vulnerabilidades de nuestras redes, sistemas y servicios.
- Realizar tareas de ciberinteligencia y cibercontrainteligencia. Será necesario disponer de los medios técnicos y humanos que permitan llevar a cabo tareas de ciberinteligencia y cibercontrainteligencia con el fin de conocer las capacidades cibernéticas propias y de los adversarios. Estas actividades permitirán, entre otras cosas, mejorar la seguridad de nuestro ciberespacio identificando aquellas vulnerabilidades que no hayan sido identificadas mediante el proceso de análisis de riesgo o conocer la tecnología utilizada por los adversarios y conocer sus vulnerabilidades para futuros ciberataques.
- Elaborar estudios y predicciones sobre las futuras capacidades TIC del enemigo enfocadas al cibercombate y operaciones de red.
- Realizar análisis forenses para dar apoyo a las ciberoperaciones y desarrollar y adaptar las nuevas tecnologías y soluciones a las tecnologías, tácticas, técnicas y procedimientos del enemigo y así poder ejecutar acciones eficaces de ciber-combate y operaciones de red.
- Mitigar o remediar las intrusiones o ataques enemigos.

CONOCIMIENTO DE CÍBERSITUACIÓN

DESCRIPCIÓN

El conocimiento de la cibernsituación es el conocimiento inmediato del ciberespacio propio o aliado, el del enemigo y el de cualquier otro de interés, así como el conocimiento del estado y disponibilidad de las capacidades de ciberoperaciones que son necesarias para el planeamiento, conducción y mando y control de las ciberoperaciones y de las operaciones en general. El conocimiento de la cibernsituación se obtiene como resultado de la combinación de actividades de inteligencia y operativas en el ciberespacio, el espacio electromagnético y en cualquier otra de las dimensiones del entorno operativo (tierra, mar, aire y espacio).

CAPACIDADES

Los procesos, procedimientos y capacidades del conocimiento de cibernsituación, deben ser desarrollados para contribuir al conocimiento de situación global del mando, así como a la consecución de sus objetivos. Las Fuerzas Armadas requerirán de las siguientes capacidades:

- Proporcionar al mando una gestión de conocimiento operativa sobre las ciberoperaciones propias o aliadas, de los adversarios o de cualquier otra parte del ciberespacio relevante para el COP del mando y que apoye sus procesos de toma de decisiones.
- Proporcionar al mando visibilidad, en tiempo real, de las redes, sistemas, servicios propios y sus dependencias.
- Proporcionar al mando visibilidad, en tiempo real, de las acciones del enemigo sobre las redes, sistemas y servicios propios, así como el posible impacto en la consecución de los objetivos operativos.
- Proporcionar al mando el conocimiento del impacto operativo de sus decisiones sobre las ciberoperaciones, contribuyendo al proceso de toma de decisiones.
- Suministrar al mando información lo más detallada posible, incluyendo información de inteligencia fundamental para apoyar el proceso de toma de decisiones acerca del ciberespacio y las ciberoperaciones.
- Coordinar y compartir esfuerzos entre los Ejércitos, la Armada, el Estado Mayor Conjunto, organismos auxiliares, aliados, la industria, contratistas y cualquier otro socio

privado o público para obtener un conocimiento de la cibersituación lo más completo posible.

- Identificar amenazas en el ciberespacio, incluyendo los adversarios potenciales, para contribuir al conocimiento de la situación (*situational awareness*) del mando y los objetivos operativos y de inteligencia.
- Estudiar las motivaciones, los objetivos y análisis de los adversarios potenciales en sus posibles decisiones para dirigir ciberataques a los intereses propios o aliados, de modo que se pueda realizar una planificación de las ciberoperaciones y operaciones militares en general.

Estado de situación del ciberespacio global de las Fuerzas Armadas españolas

En la actualidad el ciberespacio global de las Fuerzas Armadas ofrece un conjunto de servicios insuficientes para las necesidades operativas demandadas. Existen ciertas capacidades para llevar a cabo cíber-operaciones pero estas capacidades no ofrecerían un conocimiento de cibersituación completo y fiable, esencial para que el mando ejerza su función y para el éxito de las operaciones en general.

Desde el punto de vista de las TIC el grado de obsolescencia es desigual, con arquitecturas CIS no unificadas y en muchos casos no interoperables, figura 4.

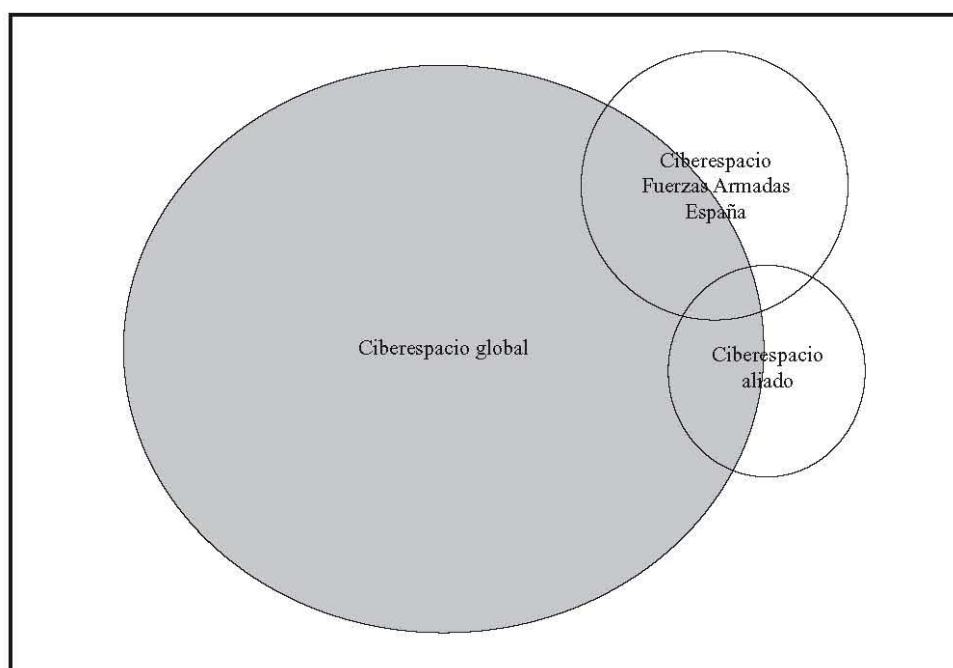


Figura 4.— *Arquitecturas CIS.*

Nuestras Fuerzas Armadas, tanto en el ámbito específico de los Ejércitos y la Armada, como en el conjunto, disponen de ciberespacios propios y, prácticamente, disjuntos entre sí. Además, la evolución actual de estos ciberespacios está siendo local, lo que favorece la segregación y falta de interoperabilidad arriba mencionada.

El ciberespacio, en su ámbito más global, ha sido creado y ha adquirido su condición de esencial para nuestra sociedad mediante la contribución de un inmenso número de entidades, ya sean individuales o colectivas (empresas, organismos y administraciones). Gracias a la continua y rápida evolución de las TIC y, en particular, a un conjunto reducido de protocolos (especialmente el IP), la suma de tales contribuciones, en su mayor parte no planificadas ni dirigidas desde uno o pocos puntos, ha dado un resultado coherente que ahora llamamos ciberespacio, en el que se pueden ejecutar acciones planificadas con efectos concretos. En definitiva, algo que ha surgido sin un gobierno único y que se ha convertido en esencial para la actividad socioeconómica actual presenta al mismo tiempo multitud de vulnerabilidades y amenazas cuyos impactos podrían ser devastadores.

Pueden identificarse dos grandes opciones para adquirir una posición de fortaleza en el ciberespacio, tanto para la defensa de los servicios propios como para el ataque sobre los de los adversarios en caso necesario. La primera opción consistiría en regular desde las administraciones públicas la construcción y explotación del ciberespacio en los ámbitos de jurisdicción propia, creando mecanismos de seguridad que asegurasen un control total del ciberespacio propio. Esta opción es la que están aplicando algunos países como China. No obstante, ha sido la escasa regulación existente hasta hace pocos años en el ámbito de Internet la que ha permitido, en gran parte, la espectacular evolución de las TIC y la constante innovación de servicios en Internet. Adoptar, por tanto, esta opción podría presentar un riesgo de desaceleración, o quizás recesión, en la importancia como factor dinamizador social, económico y cultural del ciberespacio.

La segunda opción: se centraría en implementar mecanismos que permitan la prevención y detección de ataques contra el ciberespacio propio o aliado, así como la capacidad de respuesta sobre las capacidades del ciberespacio enemigo. Esta opción es la que están siguiendo países del entorno aliado de España, como Estados Unidos o Reino Unido, y parte de la base de que el ciberespacio no puede fragmentarse en islas para protegerlo y al mismo tiempo conservarlo como motor de innovación y evolución socioeconómica. Como se ha expuesto anteriormente, la ventaja en el ciberespacio se adquiere mediante la anticipación en el análisis y gestión de riesgos y el liderazgo en la investigación y desarrollo de las TIC.

Trasladar esta segunda opción al ámbito militar español implica inmediatamente la necesidad de establecer un ciberespacio propio para Fuerzas Armadas. En definitiva, definir, implantar y gestionar un ciberespacio conjunto. La situación actual en las Fuerzas Armadas españolas es aún el de una fuerte implantación de redes y sistemas disjuntos. Cada Ejército y la Armada han impulsado programas de adquisición de capacidades CIS que han resultado en la implantación de sistemas y servicios en los respectivos ámbitos específicos. En otras palabras, se han creado ciberespacios específicos. No obstante, también permanecen programas conjuntos para dotar a todas las Fuerzas Armadas de una capacidad conjunta, de un ciberespacio conjunto. En este sentido, el concepto del Sistema de Mando y Control Militar (SMCM), en primer lugar, y el de NEC más recientemente, son iniciativas orientadas a disponer de un ciberespacio conjunto y fácilmente integrable en ciberespacios aliados.

Desde el año 2002, el Estado Mayor de la Defensa (EMAD) trabaja en la definición e implantación del SMCM, cuyo componente CIS debe ofrecer servicios de telecomunicaciones, a través del Sistema de Telecomunicaciones Militar (STM), así como un conjunto de servicios comunes (correo interpersonal, mensajería formal, ofimática, entre otras) y servicios informáticos comunes y específicos (inteligencia, logística, operaciones, cartografía militar, entre otras) a través del Sistema de Información Militar (SIM). Ambos, STM y SIM, están siendo desarrollados e implantados siguiendo los principios básicos de la seguridad de la información que garantizan la autenticidad de las comunicaciones y usuarios, confidencialidad de las comunicaciones e integridad de los datos. Además, el SMCM deberá garantizar la disponibilidad de los servicios STM y SIM, así como la trazabilidad y auditabilidad de todas las acciones ejecutadas por los usuarios del SMCM.

Sin embargo, hasta el momento, sólo se ha conseguido implantar cierta capacidad CIS conjunta, concretamente la correspondiente al enlace de los distintos emplazamientos en territorio nacional y puntos de anclaje en zonas de operaciones, además de una red IP construida a partir del servicio de mensajería formal militar del EMAD (SICOMEDE). Adicionalmente, el EMAD dispone de un Sistema de Información (SIJE) limitado en alcance prácticamente al Cuartel General del EMAD y a pocos terminales en los puestos de mando desplegados en las zonas de operaciones.

Los sistemas específicos de los Ejércitos y la Armada (SIMACET, ICC nacional, SMN, SACOMAR, etc.) se han concebido, diseñado e implantado aisladamente unos de otros y sólo comparten la capacidad de transmisión que les ofrece el STM del EMAD. No

comparten un servicio IP de red y la interoperabilidad entre ellos es mínima. En la siguiente figura se muestra una relación, no exhaustiva, de los actuales sistemas militares españoles en los ámbitos conjunto y específico (Ejércitos y Armada), con la indicación de los servicios principales que proporcionan y de la red que emplean actualmente para la interconexión de sus nodos. La Red de Propósito General (RPG) es la red del Ministerio de Defensa que tiene como objetivo el proporcionar los servicios relacionados con las funciones administrativas del Ministerio. La RPG cuenta entre sus objetivos la acreditación formal de seguridad para manejar información clasificada hasta el grado de *Difusión Limitada*.

El Ejército de Tierra y la Armada han iniciado procesos de integración de los distintos servicios existentes en sus respectivos ámbitos para la obtención de sistemas integrados que permitan una gestión corporativa de la información y los propios servicios. En otras palabras, están acometiendo procesos para la creación de un ciberespacio específico en su ámbito. Tales son los casos del SIMACET (Ejército de Tierra) y el SMN (Armada).

Es destacable el hecho de que ciertos sistemas militares están empleando las capacidades de la RPG en lugar de las del SMCM, debido a la indisponibilidad aún de un servicio de red adecuado en el STM en cuanto a alcance geográfico y capacidad de ancho de banda. Los aspectos de seguridad pueden verse comprometidos por el hecho de que la RPG aún no cuenta con una acreditación de seguridad acorde al grado de confidencialidad que requiere la información manejada por estos sistemas.

Además, según el concepto CIS del SMCM, el SIM debe proporcionar las capacidades CIS necesarias (infraestructura CIS, servicios básicos, incluidos los de seguridad para una adecuada acreditación) para la integración de todos los servicios específicos de las Fuerzas Armadas en un único sistema corporativo. Sin embargo, como se ha referido anteriormente, el SIM aún no ha sido puesto en servicio, figura 5.

Ámbito conjunto - EMAD			
Sistema	Acrónimo	Servicios	Red
Sistema de Información del JEMAD	SIJE	Comunes	SMCM (sólo transmisión)
Sistema Conjunto de la Defensa	SICONDEF	Comunes INTEL	SMCM (sólo transmisión)
Sistema de Mensajería de la Defensa	SICOMEDE	MMHS	SMCM (red IP)
Ámbito específico - Ejército de Tierra			
Sistema	Acrónimo	Servicios	Red
Sistema de Información de Mando y Control del Ejército de Tierra	SIMACET	Comunes: OPS	SMCM (sólo transmisión)
Sistema Integrado de Gestión Logística del Ejército	SIGLE	LOG	RPG
Sistema de Información de Superficie	SIS	INTEL	SMCM (sólo transmisión)
Ámbito específico - Armada			
Sistema	Acrónimo	Servicios	Red
Sistema de Mando Naval	SMN	Comunes	SMCM (sólo transmisión)
Sistema Automático de Conmutación de Mensajes de la Armada	SACOMAR	MMHS	SMCM (sólo transmisión)
Sistema de Integrado de Gestión de Material	SIGMA DOS	LOG	RPG
Sistema de Gestión Logística Integridad de la Armada	GALIA	LOG	RPG
Ámbito específico - Ejército del Aire			
Sistema	Acrónimo	Servicios	Red
<i>Interim Combined Air Operations Centre Capability</i>	ICC Nacional	OPS	SMCM (sólo transmisión)
Sistema Logístico	SL2000	LOG	RPG
Sistema Integrado de Mando y Control	SIMCA	Vigilancia aérea	SMCM (sólo transmisión)

Figura 5.— *Distintos ámbitos de las Fuerzas Armadas.*

El Ejército de Tierra y la Armada han iniciado procesos de integración de los distintos servicios existentes en sus respectivos ámbitos para la obtención de sistemas integrados que permitan una gestión corporativa de la información y los propios servicios. En otras palabras, están acometiendo procesos para la creación de un ciberespacio específico en su ámbito. Tales son los casos del SIMACET (Ejército de Tierra) y el SMN (Armada).

Es destacable el hecho de que ciertos sistemas militares están empleando las capacidades de la RPG en lugar de las del SMCM, debido a la indisponibilidad aún de un servicio de red adecuado en el STM en cuanto a alcance geográfico y capacidad de ancho de banda. Los aspectos de seguridad pueden verse comprometidos por el hecho de que la RPG aún no cuenta con una acreditación de seguridad acorde al grado de confidencialidad que requiere la información manejada por estos sistemas.

Además, según el Concepto CIS del SMCM, el SIM debe proporcionar las capacidades CIS necesarias (infraestructura CIS, servicios básicos, incluidos los de seguridad para una adecuada acreditación) para la integración de todos los servicios específicos de las Fuerzas Armadas en un único Sistema corporativo. Sin embargo, como se ha referido más arriba, el SIM aún no ha sido puesto en operación.

Conclusiones

CÍBEROPERACIONES *VERSUS* CÍBERDEFENSA

Debe superarse el concepto de ciberdefensa y evolucionar al de ciberoperaciones. El concepto de ciberdefensa está íntimamente asociado al de seguridad de la información, en el sentido de proteger la disponibilidad, integridad y confidencialidad de la misma. Las ciberoperaciones son operaciones militares que se desarrollan en el ciberespacio con los mismos objetivos que las que se producen en las dimensiones clásicas del teatro de operaciones, a saber, adquirir ventaja, conservarla y situar al enemigo en desventaja; no son solamente operaciones para proteger la información que reside en los sistemas de información, o defender los propios sistemas. Las ciberoperaciones se añaden integralmente a las operaciones terrestres, navales y aéreas para contribuir a la consecución de los objetivos del mando.

CARENCIA DE UN CIBERESPACIO ÚNICO MILITAR ESPAÑOL

La carencia de un ciberespacio militar conjunto, aparte de comprometer la acción y el mando conjuntos de y sobre la estructura operativa de las Fuerzas Armadas, supone un lastre para la adecuación o transformación de las Fuerzas Armadas para afrontar la quinta dimensión del campo de batalla, es decir, para conseguir la capacidad de planificar y conducir ciberoperaciones.

El comandante del Mando de Operaciones (MOPS), máxima autoridad operativa de las Fuerzas Armadas, necesita disponer de un conocimiento de la situación que incluya, además de las dimensiones clásicas (terrestre, marítima y aéreo), la del ciberespacio propio, el del enemigo y cualquier otro de interés operativo. Si la fuerza operativa bajo su mando emplea ciberespacios disjuntos, difícilmente se dispondrá sistemáticamente de toda la información y, mucho menos, podrán ejecutarse ciberoperaciones tanto ofensivas como defensivas.

No disponer de un ciberespacio conjunto en el ámbito de las Fuerzas Armadas españolas dificulta la planificación y ejecución de acciones de cibercombate sobre objetivos de interés, pero no impide a otros, más bien les facilita, realizar ciberoperaciones

sobre nuestros ciberespacios disjuntos, comprometiendo la capacidad militar operativa, en cualquiera de las dimensiones del entorno operativo.

ACCIONES PARA OBTENER CAPACIDAD DE CÍBEROPERACIONES

Definir un concepto de ciberoperaciones, más amplio que el actual de ciberdefensa que establezca el ciberespacio como una más de las dimensiones del entorno operativo.

Crear un mando específico para las ciberoperaciones en el seno del EMAD, u otorgar las funciones correspondientes al ya existente MOPS, que defina las necesidades operativas de la capacidad de ciberoperaciones de las Fuerzas Armadas.

Definir una estrategia de transición para alcanzar un ciberespacio militar único, o conjunto, a partir de la situación actual en la que existen varios ciberespacios específicos.

Obtener y gestionar un ciberespacio militar único. El EMAD debe implantar su concepto de SMCM, a través de programas conjuntos que aseguren la incorporación de todas las necesidades o requisitos operativos de las Fuerzas Armadas. Sólo a partir de un sistema conjunto, o sistemas específicos con el suficiente grado de interoperabilidad, puede establecerse una capacidad para planificar y ejecutar ciberoperaciones.

Fomentar y facilitar los acuerdos entre organismos públicos y el sector privado con el objetivo de dotar a las Fuerzas Armadas de un ciberespacio único y de las capacidades propias para poder llevar a cabo ciber-operaciones. Sin la implicación de la industria privada será imposible alcanzar estos objetivos.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Todo Estado debe plantearse la necesidad de proteger el ciberespacio propio con el objetivo de garantizar el desarrollo social, económico y cultural. El primer instrumento para alcanzar tal objetivo debiera ser la definición de una Estrategia Nacional de Ciberseguridad o, al menos, incluir un apartado específico sobre ciberseguridad en la Estrategia Nacional de Seguridad. Parte fundamental de la estrategia sería definir un organismo que dependiese directamente de la Presidencia del Gobierno con la misión de dirigir la ciberseguridad nacional, coordinando a las entidades públicas y privadas del país.

El ciberespacio militar es una parte más del ciberespacio global, que hay que proteger para permitir a las Fuerzas Armadas el desempeño de sus funciones. Debe iniciarse un debate sobre la conveniencia de que las Fuerzas Armadas incluyan entre sus misiones la defensa del ciberespacio nacional y el apoyo a la política internacional de España mediante el empleo de las ciberoperaciones.

Bibliografía

CLARK, Richard y KNAKE, Richard: *CYBERWAR: The Next Threat to National Security and What to Do About It*, 2010.

En: http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/ari102-2010

FOJÓN CHAMORRO, Enrique y SANZ VILLALBA, Ángel; «Ciberseguridad en España: Una propuesta para su gestión», *ARI*, número 102, , Real Instituto Elcano, 18 de junio de 2010.

STIENNON, Richard: *Surviving Cyberwar*, Govint Press, 2011.

TRADOC Pamphlet 525-7-8. US Army, febrero de 2010.

ÁNGEL SANZ VILLALBA
Ingeniero de Telecomunicaciones

ENRIQUE FOJÓN CHAMORRO
Ingeniero Superior en Informática

CONCLUSIONES

Espero que, según ha sido nuestra intención, de la lectura de las distintas aportaciones que les hemos presentado, hayan obtenido, cuando menos, algunas ideas que les permitan interpretar cómo ha podido ir adaptándose la utilización del uso de la Fuerzas Armadas por parte de los países de nuestro entorno, siempre liderados por Estados Unidos, a los cambios en la forma de hacerles frente por parte de los que, en los enfrentamientos de los últimos años, han sido nuestros oponentes y, así mismo, hayan podido asumir cómo en el futuro, las distintas formas de asimetría, de las que les hemos presentado la que podríamos considerar como una de ellas, van a seguir siendo un reto permanente a nuestra capacidad de adaptación.

Para facilitarles esa interpretación yo señalaría las siguientes conclusiones de los trabajos aportados:

- Pueden considerarse como hitos que marcan un camino en la forma de hacer la guerra en los últimos 20 años, los siguientes: 9 de noviembre de 1989, caída del muro de Berlín; 11 de septiembre de 2001, ataque terrorista a las Torres Gemelas y 15 de septiembre de 2008, quiebra del banco de inversiones Lehman Brothers, que representan: el fin de la guerra fría, el comienzo de la «guerra global contra el terrorismo» y por último el comienzo de un empleo mucho más selectivo de la fuerza ante las serias dificultades económicas.
- El primer periodo se caracteriza por un vacío estratégico en el que la idea que se impone es la Revolución en los Asuntos Militares (RMA) que prometía victorias rápidas, decisivas y sin apenas daños colaterales, gracias al empleo de una fuerza conjunta muy tecnificada y con un total conocimiento del entorno positivo.

- La RMA constituyó el paradigma de las Operaciones Basadas en Efectos (EBO) que permitiría disipar la «niebla» de la guerra y, que se consolidó, tras las operaciones aéreas en Kosovo. La consolidación se basó en un impulso *top-down* y respaldó una cierta soberbia occidental en la que los problemas de la guerra tenían una solución, cara en tecnología, pero barata en vidas propias y ajenas. Predispuso a una política de abuso en el empleo de las capacidades militares en cualquier circunstancia, como elemento de política exterior con unos costes políticos, económicos y sociales perfectamente asumibles por sus opiniones públicas.
- Para conquistar la RMA, que sentaría las bases de la guerra en red (*network centric warfare*), se juzgó imprescindible la adquisición de las novedosas tecnologías propias de la Era de la Información, así como el desarrollo de nuevas formas de actuación tales como la acción conjunta-combinada, la utilización de las EBO, rápidas y decisivas, la orientación expedicionaria, y el comienzo de la guerra espacial y ciberespacial.
- Además de los aspectos tecnológicos se aplicaron nuevos modelos de organización mediante: la generación de fuerzas modulares muy flexibles y fácilmente desplegadas, la racionalización de estructuras, nuevos modelos de adiestramiento, descentralización del mando, nueva organización de los estados mayores y un mayor control estratégico y político de las operaciones.
- Se trataba de confeccionar un catálogo de capacidades militares apropiado para actuar en toda la gama de operaciones y derrotar a cualquier potencial adversario presente o futuro. Para ello se iniciaron nuevas fórmulas de planeamiento de la Defensa, el planeamiento por capacidades, y en general se dio pie a un proceso de *transformación* que se extendería por todo Occidente.
- Los ataques del 11 de septiembre de 2001 rompen con el idílico mundo señalado por Francis Fukuyama en su «Final de la Historia» al revelar algunos de los nuevos riesgos y amenazas a la seguridad global y acabar con las proclamas »revolucionarias» de la década anterior y se consolida el movimiento de *transformación* iniciado tras la llegada al poder de la administración Bush. Con los ataques a las Torres Gemelas este proceso de Transformación se convierte en un imperativo estratégico para adaptar los ejércitos modernos al mundo del Tercer Milenio.
- España no fue ajena a este movimiento, de manera que a pesar de que el excesivo conservadurismo militar en las décadas de los años ochenta y noventa habían obstaculizado un adecuado desarrollo estratégico acorde con lo que estaba sucediendo en su entorno, la Revisión Estratégica de la Defensa primero y la promulgación de la

nueva ley de la Defensa Nacional después, permitieron subirse al carro de la *transformación* y hablar hoy con el mismo lenguaje estratégico que sus aliados.

- Inicialmente, las espectaculares victorias cosechadas por la fuerza de la coalición, especialmente la norteamericana, durante la invasión de Afganistán e Irak, asombraron al mundo pues mostraban un potencial militar occidental que parecía no tener límites. Sin embargo, entre las razones de estos éxitos se hallaban las semillas de los posteriores fracasos.
- En este periodo de fervor «revolucionario» fueron pocos los estrategas que alertaron de la excesiva confianza en la tecnología o de la posible limitación de la RMA en escenarios irregulares, nadie intuyó que una forma de lucha tan arcaica y simple como la guerra irregular revelaría los límites del estilo militar «posrevolucionario».
- El estallido de la insurgencia en Afganistán e Irak cogió desprevenido al grueso de la comunidad estratégica mundial puesto que pocos comprendían cómo una simple guerra de guerrillas podía poner en jaque a los poderosos ejércitos de Occidente. Se produce entonces un proceso *bottom up* en el desarrollo de las conocidas como operaciones Contrainsurgencia (COIN) que surge de las propias unidades como adaptación a las nuevas circunstancias.
- El auge de la insurgencia no sólo puso de manifiesto las limitaciones de la RMA en escenarios de baja o media intensidad sino también las grandes dificultades políticas, estratégicas y operativas que se entraña la estabilización de zonas hostiles y los enormes costes humanos, materiales y políticos que conllevan las campañas de cambio de régimen y reconstrucción nacional. Estos factores provocaron la desaparición definitiva de la RMA y comportaron un cambio de rumbo en el proceso de *transformación* militar.
- Se procedió a desarrollar las capacidades necesarias para combatir la amenaza irregular o asimétrica, conducir operaciones de contrainsurgencia y realizar labores de estabilización, seguridad, control del territorio o apoyo a los actores civiles en el marco de un enfoque integral a la gestión de crisis.
- Tras la guerra entre Israel y *Hezbollah* se consolida el concepto de guerra híbrida, nacido de las tácticas empleadas por la insurgencia chechena contra el ejército ruso. La amenaza híbrida se fundamenta en las posibilidades que brinda la globalización y el libre acceso a las tecnologías avanzadas y se caracteriza por la plena integración de procedimientos convencionales con tácticas propias de la guerra irregular, el empleo de

tecnologías avanzadas, la eficaz utilización de la dimensión propagandística e informativa y el desprecio a los usos y costumbres de la guerra para tratar de infligir el mayor daño posible al adversario.

- El renovado interés político, militar y académico por la guerra asimétrica, el conflicto de baja intensidad o el planeamiento de la defensa de contingencia, relegaron a un lugar secundario otros riesgos más tradicionales que estaban surgiendo durante este periodo y que no serían integrados en el pensamiento estratégico de Occidente hasta fechas recientes: el peligro de un Pakistán fallido, el arma atómica norcoreana, la proliferación nuclear Iraní, la capacidad anti satélite china, la ciberguerra sobre Estonia o la guerra convencional entre Rusia y Georgia.
- El último acaecimiento de nuestra historia, la quiebra de Lehman Brothers, marca una nueva etapa caracterizada por la frugalidad económica, el control del gasto y la escasez de recursos. Mientras la crisis económica ha provocado la contracción del gasto militar y las largas campañas han revelado los costes políticos, económicos, humanos y materiales de la guerra y la ilusión de las operaciones de construcción nacional y las dificultades de las operaciones de cambio de régimen; la *transformación* se ha reafirmado como el pilar del planeamiento de la defensa occidental y el análisis estratégico ha identificado nuevos riesgos, nuevas amenazas y ha constatado nuevas áreas de potencial conflicto.
- La inclusión de nuevos riesgos y amenazas de distinta naturaleza, procedencia y alcance en la agenda estratégica occidental, ha supuesto un importante baño de realismo que no sólo ha motivado el resurgimiento del análisis político-estratégico, sino también ha recordado a las potencias, que si pretenden continuar siendo relevantes en los asuntos globales, no sólo tendrán que prepararse para luchar en toda la gama de las operaciones sino también en garantizar la supremacía convencional frente a cualquier adversario avanzado y por lo tanto tendrán que dominar la esfera informativa, cibernética y espacial.
- Resulta necesario prestar especial atención a las distintas formas de manifestación de la asimetría en la confrontación armada ya que constituyen un elemento de especial riesgo para la seguridad. En este sentido, requiere una especial atención la ciberdefensa, ya que puede ir dirigida hacia cualquier estamento del Estado sin aviso previo y con efectos que pueden llegar a ser nocivos para su normal funcionamiento.
- En España, la fragmentación en la responsabilidad en materia de seguridad, respecto a posibles ataques cibernéticos, representa un elemento de debilidad que exige la

existencia de un organismo de coordinación que, mediante una visión global, permita desarrollar una estrategia de ciberdefensa de carácter nacional.

- En el ámbito exclusivo militar el no disponer de un ciberespacio conjunto dificulta la planificación y ejecución de acciones de cibercombate sobre objetivos de interés y facilita, a los posibles oponentes, la realización de ciberoperaciones que comprometan nuestra capacidad militar.
- El comandante del mando de operaciones debe asumir el mando de las ciberoperaciones y el jefe del Estado Mayor de la Defensa establecer los programas que aseguren la incorporación de todas las necesidades y requerimientos operativos de las Fuerzas Armadas en esta área.

JOSÉ MARÍA TERÁN ELICES
Almirante (R)

COMPOSICIÓN DEL GRUPO DE TRABAJO

Presidente-coordinador: D. JOSÉ MARÍA TERÁN ELICES
Almirante (R).

Vocales: D. ENRIQUE FOJÓN LAGOA
Coronel de Infantería de Marina (R).

D. GUILLEM COLOM PIELLA
Doctor en Seguridad Internacional.

D. ÁNGEL SANZ VILLALBA
Ingeniero de Telecomunicaciones.

D. ENRIQUE FOJÓN CHAMORRO
Ingeniero Superior en Informática.

Las ideas contenidas en este trabajo son de responsabilidad de sus autores, sin que refleje, necesariamente el pensamiento del CESEDEN, que patrocina su publicación