CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

FUNDACIÓN SAGARDOY

MONOGRAFÍAS

del

CESEDEN

94

CÁTEDRA «MARQUÉS DE SANTA CRUZ DE MARCENADO»

TECNOLOGÍA Y FUERZAS ARMADAS

MINISTERIO DE DEFENSA

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

FUNDACIÓN SAGARDOY

MONOGRAFÍAS

del

CESEDEN

94

CÁTEDRA «MARQUÉS DE SANTA CRUZ DE MARCENADO»

TECNOLOGÍA Y FUERZAS ARMADAS

Febrero, 2007

TECNOLOGÍA Y FUERZAS ARMADAS

SUMARIO

PRÓLOGO

PRÓLOGO

Por ÁNGEL MONTOYA CEREZO

La aplicación de la tecnología al servicio del arte de la guerra es algo intrínseco al hombre. Ya desde los primeros tiempos el arco servía para combatir o para cazar, siendo así una tecnología de "doble uso". Quiere decir eso que la tecnología y la defensa han estado desde siempre imbricadas y que las capilaridades de las aplicaciones militares a civiles y las civiles a militares han sido una constante que han discurrido en paralelo.

La evolución que han experimentado los conflictos con la irrupción de nuevas formas de concebir la acción violenta o agresora, origina que los gobiernos se decanten, no sólo por las inversiones en desarrollos tecnológicos en los campos tradicionales, sino en aquellos que van a proporcionar una clara supremacía en el combate ante los peligros potenciales del terrorismo.

Las agencias de investigación avanzada u observatorios tecnológicos dependientes de los Ministerios de Defensa, pretenden armonizar las necesidades de las Fuerzas Armadas y las disponibilidades presupuestarias priorizando aquellas inversiones que se consideran importantes por razones técnicas, económicas o de conveniencia estratégica para el país.

Hace años los presupuestos dedicados a Investigación y Desarrollo (I+D) de los Ministerios de Defensa superaban con creces a las inversiones que podían hacer las grandes empresas con cargo a sus cuentas o los que se subvencionaban desde el resto de los organismos de la Administración para aplicaciones civiles. Esto hacía que los equipos y sistemas militares evolucionaran tecnológicamente de manera más rápida que los civiles. Hoy en día los mercados civiles se ven apoyados por las economías de consumo y los grandes mercados que permiten optimizar las inversiones a corto plazo en base a un mercado de cientos o miles de millones de clientes potenciales.

*La utilización de elementos comerciales COTS (*Comercial on the Shelf*) en los grandes sistemas militares hace que se replantee la estrategia de las Administraciones centrales y de las empresas, dedicando su capacidad de I+D a aquellas áreas donde no llega el mercado civil o donde es necesaria la particularización de los logros alcanzados en ese mercado.*

Desde hace siglos la supremacía tecnológica ha sido un factor importante en la consecución de los éxitos militares y en el dominio de los escenarios del conflicto, pero no sólo en situaciones de crisis o guerra abierta, sino también en escenarios de conflicto sin guerra declarada y situaciones prebélicas. Actualmente las Fuerzas Armadas evolucionan en sus cometidos realizando no solo labores puramente bélicas, si no también labores de policía en los territorios que ocupa.

Hoy en día las mafias y bandas organizadas disponen de tecnologías avanzadas que requieren de sistemas complejos por parte de las policías que los combaten y estos sistemas se aproximan cada vez más a los utilizados hasta ahora por las Fuerzas Armadas.

Vemos que algunas labores de los ejércitos se acercan a las de las Fuerzas de Seguridad y a su vez, las de las Fuerzas de Seguridad se aproximan a las puramente militares. Lo mismo puede decirse de ciertas funciones asumidas por las Fuerzas Armadas que han sido clásicamente encomendadas a los servicios de Protección Civil. Todo ello sigue confirmando la aproximación y la convergencia de tecnologías entre las actividades civiles y militares.

La tecnología militar ha de transformarse con las tipologias de conflictos que van apareciendo. En este sentido, se ha acuñado hace unos años el término de guerra asimétrica. El término es relativamente nuevo pero no el concepto. La palabra "guerrillero" nace en España en los enfrentamientos asimétricos contra Napoleón pero es, incluso, anterior a esta época en lo que a concepto se refiere.

*Puede ser que cuanto más armado esté un país y mayor sea la supremacía que alcanza, más obligue a su enemigo a buscar capacidades tecnológicas baratas pero eficaces y que puestas a su servicio pueden ser de un efecto atroz en comparación con las inversiones llevadas a cabo. Usará Internet, localizadores GPS (*Global Positionnig System*), telefonía móvil celular o vía satélite, sistemas inalámbricos,*

encriptación etc. Sistemas comunes al servicio de la sociedad pero también de los potenciales enemigos. Nace así la metodología no tradicional o no convencional de hacer la guerra que busca evitar las fortalezas del enemigo y explotar las vulnerabilidades sin recurrir a un enfrentamiento tecnológico directo que le abocaría al fracaso.

Los ejércitos tienen que adaptarse continuamente a las nuevas formas de la guerra. Los actos de terrorismo son claro ejemplo de ello pero, es difícil prever esas nuevas formas. El enemigo empleará todos sus recursos en descubrir aquellos actos o procedimientos, que representen su mayor beneficio por el impacto que generan y que signifique la mayor sorpresa. Será labor de las Fuerzas Armadas descubrir esas iniciativas e introducirse en el núcleo de toma de decisiones del enemigo.

Las Fuerzas Armadas de los países que soportan actos de terrorismos pueden permanecer indemnes tras estos hechos, pero las consecuencias en la población son tremendas. Se produce miedo colectivo, se incrementan las medidas de seguridad, se restringe la movilidad de las personas, se desconoce el causante y sus pretensiones, si la acción ha finalizado o es sólo el principio, etc.

Las cabezas visibles de los potenciales enemigos serán claramente identificadas unas veces y otras serán difusas no permitiendo combatirlas frontalmente. Unas veces el enemigo estará en nuestro territorio, oculto y latente, y otras muy apartado de él. Todos los sistemas de inteligencia toman relieve en este caso para la obtención de información y la previsión de las posibles acciones ofensivas.

El acceso a la información, su intercambio y la capacidad de procesarla será una tecnología importante en los próximos tiempos para anticiparse en lo posible a los nuevos retos.

Se pretende con este libro dar un repaso a la situación tecnológica de España, sus relaciones internacionales desde ese punto de vista, las necesidades presentes de las Fuerzas Armadas y la evolución futura, intentando cubrir los diferentes puntos de vista y las expectativas de los actores implicados en el amplio concepto de tecnología y Fuerzas Armadas.

CAPÍTULO PRIMERO

ANTECEDENTES

ANTECEDENTES

Por JUAN M. ORTI PÉREZ

Algunos autores datan el origen de la tecnología en su carácter militar o de defensa en los tiempos primitivos en los que los primeros pobladores de la Tierra descubrieron que los objetos punzantes o cortantes eran más capaces de producir una herida que otros que no disponían de esta característica. La acumulación de experiencia y de conocimientos permitió la evolución de estas rudimentarias armas hacia diseños más elaborados.

No es nuestro propósito entrar en detalles sobre dicho origen, ni siquiera describir la evolución de la tecnología militar desde aquellas primitivas armas hasta nuestros días, sin embargo, sí que hemos considerado de interés dedicar este capítulo a los antecedentes inmediatos a la situación actual que se estudia en los capítulos siguientes, para ello hemos tomado como punto de partida el final de la Segunda Guerra Mundial, momento en que la aparición del transistor revolucionó el campo de la electrónica y dio paso a lo que muchos autores han denominado la “era de la automatización”.

Al tiempo que la tecnología se hacía cada vez más compleja en los años de la posguerra mundial y los ejércitos pasaban a un periodo de paz, la burocracia se fue incrementando y sus estructuras fueron alterándose en el sentido de disminuir las unidades de combate y aumentar las de servicios y auxiliares. Al mismo tiempo fueron creciendo el número de departamentos, secciones, ramas, especialidades y otras subdivisiones.

Este incremento de la complejidad de las estructuras orgánicas y operativas que dificultaba el ejercicio del mando llevó a una reducción de la entidad de las unidades y a un incremento de la de los órganos de mando. De este modo, la tecnología dio

paso a la complejidad, la complejidad a una extraordinaria necesidad de información, y ésta a su vez a un enorme papeleo ([1]).

Esta invasión de la burocracia podía haber bloqueado al ejército más avanzado de no haber sido por la aparición en escena de los equipos mecánicos de procesado de datos. Una vez más, se trataba de una innovación aparecida en el campo militar. Sus precursores fueron las cintas perforadas utilizadas ya desde principios del siglo XX.

Los rudimentarios procesadores de datos fueron empleados para investigación aeronáutica y para el cifrado y descifrado de mensajes durante la segunda Guerra Mundial (procesadores “Ultra”, “Bomba”, “Enigma”, “Magic”), avances que sin duda tuvieron una notable influencia en el desarrollo de los acontecimientos bélicos.

Otro uso militar del procesado de datos se dio en la defensa aérea. En este campo, todo dependía en aquellos años de la coordinación entre radares, proyectores, artillería antiaérea y aviación de combate, una tarea que había de llevarse a cabo con rapidez y precisión. Para ello se utilizaron calculadoras mecánicas y electromecánicas con las que se pretendía dotar al sistema de capacidad para identificar la aeronave hostil, hacerle el seguimiento, determinar sus datos de vuelo y abatirla. La guerra terminó antes de que se consiguiera la completa integración de los diferentes elementos del sistema, sin embargo, quedaban dados los primeros pasos para su completa automatización.

Para Van Creveld, que ha dedicado muchas de sus obras al estudio de los avances tecnológicos al compás de la evolución del arte de la guerra, las calculadoras fabricadas y empleadas durante la Segunda Guerra Mundial tenían dos importantes inconvenientes. El primero que se formaba de un gran número de componentes móviles, lo que significaba una gran complejidad y una alta relación peso/potencia del conjunto, para una baja velocidad de cálculo. El segundo consistía en que su falta de capacidad para elegir entre operaciones alternativas (capacidad conocida como *branching*) les impedía llegar a considerarse verdaderos ordenadores.

---

[1] VAN CREVELD, Martin. Tecnology and War. The Free Press. New York, 1991. Pg 237.

El primero de esos problemas lo resolvió J. Presper Eckbert en el año 1946 con la invención del ENIAC (*Electronic Numerical Integrator and Calculator*) en el que reemplazaba las ruedas dentadas por circuitos electrónicos, aunque todavía muy rudimentarios.

El segundo de los problemas fue resuelto por John von Neumann en el año 1947 con la invención de la programación almacenada ([2]). Este primer programa de ordenador de Neumann se podía almacenar en la memoria y contenía instrucciones para realizar diversas operaciones matemáticas. Además, era capaz de tomar decisiones en función del resultado de sus cómputos mediante secuencias de operaciones diferentes. Fue utilizado en el cálculo de tablas de tiro, en el diseño de armas y aeronaves, en la gestión de personal y en el control de inventarios.

La aparición del transistor en el año 1947 supuso un notable avance en el campo de la electrónica. En los años cincuenta, el transistor comenzó a reemplazar al tubo de vacío. Años más tarde el circuito integrado de materiales semiconductores se impuso, permitiendo una notable reducción del tamaño y peso de los aparatos. De igual manera se avanzó en el desarrollo de *software* y de equipos periféricos y los costes se redujeron significativamente.

Toda esta evolución de los sistemas de cálculo –es preciso recalcarlo- estuvo íntimamente ligada desde el principio al mundo militar, en concreto en Norteamérica, no sólo en el diseño y desarrollo de la tecnología sino también en la financiación de los proyectos y en el consumo y utilización de los equipos y componentes resultantes. Posiblemente, los motivos hubiera que buscarlos en el tamaño de la organización militar en comparación con otras organizaciones de carácter civil de la época y la necesidad de gestionarla y administrarla eficazmente; y en la necesidad de simplificar el ejercicio del mando y las comunicaciones en combate para contrarrestar la complejidad de la guerra.

Durante los años cincuenta los objetivos buscados por la automatización se centraban en aspectos de administración de los recursos humanos, archivos, y

---

[2] VAN CREVELD, Martin. Tecnology and War. The Free Press. New York, 1991. Pg 238 y sigs.

aspectos logísticos tales como petición y seguimiento de piezas y repuestos. Todo ello en aras de rentabilizar lo que ya se conocía como el “binomio coste/eficacia”.

El impacto tecnológico de los ordenadores que se iniciara en estos aspectos administrativos y logísticos, pronto alcanzó el mundo de las comunicaciones, en el que permitió pasar de interruptores y cuadros de mandos manuales y mecánicos a otros completamente automáticos y electrónicos. Durante la guerra de Vietnam ya se utilizaban sistemas de comunicaciones completamente automáticos soportados por equipos de pequeño volumen, robustos y altamente fiables.

Los sistemas de comunicaciones integrados fueron utilizados a su vez para interconectar los ordenadores de diferentes estamentos de la organización, permitiendo una significativa reducción de personal.

Al final de la década de los sesenta, se consiguió enlazar los ordenadores –mediante cable y sin él- a una gran variedad de sensores electrónicos tales como cámaras de televisión, radares, sonares, etc. Este nuevo tipo de interconexiones, utilizado sobre el terreno, sobre buques, sobre aeronaves, o sobre satélites, abrió un nuevo campo de posibilidades a la inteligencia militar, permitiendo al mando militar disponer de información actualizada de gran valor para su toma de decisiones.

Pero en el campo de la inteligencia los ordenadores llegaron mucho más allá, una vez que se les dotó del adecuado *software*, ya que se consiguió que clasificaran las señales de acuerdo con unos criterios preestablecidos, asumiendo de esta manera algunas de las funciones que llevaban a cabo hasta entonces los analistas de inteligencia. Además, si el ordenador era capaz de identificar una amenaza, también lo sería de activar la correspondiente alarma y de hacer reaccionar el sistema de armas adecuado para dar respuesta automática prescindiendo de la mano del operador.

También es cierto que la evolución de la guerra durante las décadas que nos ocupan hicieron tan complejas las formas de combate, que no siempre la más avanzada tecnología permitía la resolución inmediata de los problemas. Ello no fue obstáculo para que se desarrollaran dos importantes innovaciones en el campo de la automatización en la década de los años sesenta.

El primero fue el sistema de misil guiado ligado al radar, que luego se mostró muy efectivo en la guerra árabe-israelí del Yom Kippur de 1973, en la que fue desplegado en los Altos del Golán por los árabes y causó numerosas bajas en la aviación israelí, aunque también derribó algún aparato sirio. Se trataba de los misiles SAM-2 de alta cota, los SAM-3 *Goa*, y los SAM-6 *Gainful* de fabricación soviética, que hicieron estragos en la aviación israelí hasta que los *Phantom* facilitados por los norteamericanos comenzaron a montar las correspondientes contra-medidas ([3]).

El segundo fue el misil estratégico con cabeza nuclear basado en tierra, que no llegó a ser dotado de una automatización completa por los riesgos que suponía una falsa alarma o un error mecánico para una escalada de los acontecimientos.

Pero no siempre se conseguía en la práctica la adecuada relación coste-eficacia, a la que antes aludíamos, en los campos de las comunicaciones, de la inteligencia, de la administración o de las operaciones, debido fundamentalmente al elevado coste de los ordenadores. La excesiva centralización del mando y de la gestión, consecuencia del buen funcionamiento de las comunicaciones, multiplicó las consecuencias del error humano, dilató los periodos de reacción y encorsetó la iniciativa y la libertad de acción en los escalones más bajos.

No fue eso todo. La razón fundamental para que se introdujera el uso del ordenador en el campo militar y se fomentara su uso en red, había sido la enorme cantidad de información que se necesitaba manejar por las Fuerzas Armadas modernas en el entorno creado por la guerra del momento. Pues bien, una vez que los ordenadores y las redes que los enlazaban estaban en disposición de operar de forma eficaz, se incrementó enormemente la cantidad de información a procesar. Para reducirla hasta niveles asimilables por el mando militar fue necesario incrementar los cuarteles generales y los estados mayores, quienes pronto pidieron ser dotados de sus correspondientes ordenadores. Se entró así en una espiral a la que no se veía fin.

Tanto entonces como ahora, es preciso determinar cuales son los campos de trabajo y la cantidad de éste que ha de ser asignado a los ordenadores. Es lo que Van

---

[3] BARKER, A.J. La Guerra del Yom Kippur. Editorial San Martín. Madrid, 1975. Pgs 112 y sigs.

Creveld define como “modelar” y “cuantificar” las áreas a las que tendrán que hacer frente ([4]).

Durante la guerra de Vietnam y en los años posteriores a ella no faltaron voces en Estados Unidos que achacaron sus dudosos resultados a la tecnología militar, que consideraban inadecuada para ese tipo de guerra. Aunque los argumentos de quienes la criticaban no eran del todo ciertos, sí se podría decir que el análisis de la estrategia utilizada por los americanos fue reducido casi exclusivamente a términos cuantitativos. La concepción de las operaciones descansaba en exceso en los ordenadores y era más relevante un gráfico de bajas o una tabla estadística que la moral de las tropas o que cualquier otro factor no cuantificable.

En los años ochenta parecían haberse asimilado aquellos errores de la guerra de Vietnam. La informática continuaba su imparable desarrollo especialmente en lo que afectaba a la reducción de tamaño de los componentes y al aumento de potencia, lo que permitió su uso en campaña y, por tanto, su implantación en toda la infraestructura de la guerra, hasta llevar el día a día de los ejércitos a depender plenamente de ella.

Simultáneamente a este desarrollo apareció una corriente de militares “reformistas” que pretendía poner sobre aviso de la excesiva dependencia de la informática en el campo militar y sugería reflexionar sobre el asunto. Para ellos, independientemente de lo que dijeran los analistas de sistemas y los defensores de la teoría de juegos, la guerra representaba una ciencia por sí misma y no podía ser reducida a cualquier otra. Los principios de dicha ciencia se basaban en la historia militar y en los textos clásicos y no podían simplemente ser una adaptación de los tecnológicos. Basada en parte en la influencia de estos reformistas se abrió paso en Estados Unidos una nueva forma de entender las operaciones militares conocida como “guerra de maniobra”, que se implantó como una filosofía de combate que busca destruir la cohesión del adversario mediante una serie de acciones rápidas, violentas e inesperadas que produzcan un deterioro rápido y turbulento de la situación a la que aquél no puede hacer frente. Aunque los ordenadores continuaban siendo utilizados

[4] VAN CREVELD, Martin. Tecnology and War. The Free Press. New York, 1991. pg 243

para simulaciones tácticas y para el análisis de problemas, parecía abrirse un nuevo campo de trabajo para ellos, en el que se equilibraba el peso de la tecnología y el arte de la guerra.

Si los ordenadores supusieron un hito en la historia de la tecnología, derivado de la Segunda Guerra Mundial, la energía nuclear constituyó otro punto de inflexión, con mayor incidencia aún en los asuntos militares. Los trabajos realizados por Planck, Einstein, Schroedinger y otros, a principios del siglo XX, tras el descubrimiento de la radiactividad por Becquerel en 1896, no fueron comprendidos en toda su magnitud –al menos en lo que a aplicaciones militares se refiere- hasta finales de los años treinta, en que Alemania comenzó las investigaciones atómicas de aplicación militar. Estados Unidos pronto tomó el relevo y en 1941 realizó un extraordinario esfuerzo en este campo, que le situó muy por delante de cualquier otro país y le permitió fabricar las primeras bombas atómicas, cuyos devastadores efectos fueron puestos de manifiesto en agosto de 1945 en Hiroshima y Nagasaki.

En el mismo momento en que se empleó la bomba nuclear surgió un intenso debate sobre su uso. La cuestión se centraba en si se debía considerar el arma nuclear como un arma más en el escenario bélico o si, por el contrario, su uso racional debía limitarse a la prevención de la guerra y la disuasión.

Sin entrar en cuestiones polemológicas sobre el uso del arma nuclear, que no son objeto de este trabajo, sí es preciso decir que ha sido protagonista principal y factor fundamental en la estrategia de los dos bloques durante la guerra fría, como más tarde veremos. La llamada “estrategia de disuasión” se basaba en influir directamente en la voluntad del adversario sin el paso intermedio de una prueba de fuerza.

Los aspectos tecnológicos del desarrollo de las capacidades del arma nuclear pueden analizarse considerando el artefacto explosivo y su producción, la plataforma de lanzamiento y las medidas defensivas adoptadas por el enemigo:

- Primero fue la bomba de fisión nuclear, cuyo funcionamiento se basa en la escisión de un núcleo pesado (de uranio-235 en el caso de la bomba de uranio, o de plutonio-239 en el caso de la bomba de plutonio) en elementos más ligeros

mediante el bombardeo de neutrones, que al impactar en dicho material provocan una reacción nuclear en cadena. Más tarde se dio un paso importante en los avances del arma nuclear con el desarrollo de la “bomba de hidrógeno”, también llamada “nuclear de fusión” o “termonuclear”, utilizada por primera vez en el año 1952. A diferencia de sus predecesoras basaba su efecto en la fusión en lugar de la fisión, esto es, en la fusión de núcleos ligeros (isótopos del hidrógeno) en núcleos más pesados, en lugar de la fisión de los núcleos atómicos. Su aparición significó un salto cuantitativo de gran importancia en la producción de armas nucleares. En cuanto a la evolución del arma, los esfuerzos de los científicos y técnicos en armamento se centraban por aquellos años en fabricar ojivas de baja capacidad que pudieran ser empleadas de forma selectiva incluso cerca de las tropas propias sin producirles bajas y sin desencadenar la escalada de la crisis nuclear; maximizar los efectos minimizando la radiación; y lo que tecnológicamente era más complicado, la miniaturización de los componentes.

- La miniaturización del arma llevó a la simplificación y diversificación de las plataformas, de manera que su lanzamiento llegó a poder realizarse desde cazabombarderos o desde simples vehículos de ruedas, bajo la forma de misil táctico, misil de crucero o simple proyectil de artillería. Estas plataformas y vectores además, conseguían con el tiempo mayor precisión sobre el blanco.

- En cuanto a las medidas defensivas, en los años cuarenta y cincuenta fueron objeto de un importante desarrollo las tecnologías dedicadas a la alerta temprana y a los sistemas de defensa antiaérea, si bien no fueron suficientes para garantizar un mínimo de seguridad frente a los Misiles Balísticos Intercontinentales (ICBM) que comenzaron a estar operativos a principios de los años sesenta.

En cualquier caso, durante los años de la guerra fría, el desarrollo tecnológico del arma nuclear, la estructura de las fuerzas y la ubicación de los sistemas de armas estuvo marcado por las diferentes percepciones de su posible uso que desde cada uno de los lados del “telón de acero” se tenían y los diferentes enfoques de la prevención de un ataque proveniente del otro lado.

Fue el temor a una “destrucción mutua” el que llevó a ambos bandos a tomar medidas preventivas de una escalada nuclear, como la puesta en servicio del “teléfono rojo” o la firma de acuerdos limitativos de armas estratégicas ([5]); y fue precisamente el desarrollo de los sistemas defensivos el que condujo a una carrera que más tarde la Unión Soviética no podría resistir.

Los Acuerdos SALT-I reflejaban lo que era la tecnología de los sesenta. En aquellos años se pensaba que la capacidad misilística de cada uno de los bandos era invulnerable a un primer ataque, debido al empleo de submarinos y plataformas móviles que permitían dispersar y ocultar las ojivas, e incluso protegerlas, dificultando su destrucción para poder responder a un primer ataque manteniendo su capacidad disuasoria. Pronto los avances tecnológicos echarían por tierra estas creencias. El más importante de ellos –no regulado por el SALT que sólo limitaba el número de misiles y no el de cabezas nucleares- fue el desarrollo en la década de los setenta de misiles dotados de varias ojivas que, aunque más pequeñas, se separaban en la última fase de la trayectoria hacia el blanco, aumentando su poder destructivo. Estas ojivas se perfeccionaron con sistemas de corrección de la trayectoria una vez escindidas del cuerpo principal, lo que permitía ataques más precisos que se podían dirigir contra los silos del adversario y conservar una importante capacidad de respuesta. El sistema resultante, denominado MIRV (*Multiple Independently Targetable Reentry Vehicle*) podía ser proyectado en un único misil ICBM o en un SLBM (*Submarine Launched Ballistic Misile*) y reducía considerablemente la efectividad antimisil enemiga basada en la interceptación de misiles unitarios. La combinación de la alta precisión del MIRV con el desequilibrio que se producía entre sistema atacante y sistema defensor ponía en peligro la supervivencia de las fuerzas de segunda respuesta, o al menos de las basadas en tierra.

El segundo en importancia de los desarrollos tecnológicos que pusieron en cuestión la fuerza de ICBM del lado contrario fue la aparición del misil de crucero. Estos misiles, que habían sido desarrollados por los alemanes en la Segunda Guerra Mundial y experimentados más tarde por las Fuerzas Armadas de otras naciones, no

[5] Acuerdos NTBT (Nuclear Test Ban Treaty), SALT (Strategic Arms Limitation Treaty) y otros.

se consideró inicialmente que ofrecieran grandes ventajas frente a los ICBM y a los bombarderos. Sin embargo, durante los años setenta, los desarrollos tecnológicos permitieron fabricar pequeñas aeronaves no tripuladas, impulsadas por motores de reducido tamaño, capaces de transportar una carga útil a más de 2.000 kilómetros de distancia.

Años más tarde estos misiles de crucero serían capaces de volar a ras de suelo para violar los sistemas de vigilancia radar e incluso memorizar la trayectoria a seguir y navegar –mediante un sistema autónomo- comparando el terreno con el mapa digital residente en el ordenador de a bordo. La precisión que se alcanzó con el desarrollo de estos “misiles inteligentes” permitía destruir los misiles del adversario en sus silos e incluso acertar en sus centros de mando y control. La utilización de diferentes tipos de plataformas añadido a las cualidades antes citadas, permitía que estos misiles fueran difíciles de localizar y, por lo tanto, casi invulnerables a un primer ataque.

Estos avances en el desarrollo tecnológico de los misiles tuvieron, naturalmente, una gran influencia en la estrategia de las potencias enfrentadas durante toda la guerra fría. A la teoría inicial según la cual un primer ataque empleando bombarderos y posteriormente submarinos nucleares podía inutilizar todas o la mayor parte de las armas nucleares enemigas sucedió la de Destrucción Mutua Asegurada (MAD), según la cual, cualquier uso de armamento nuclear por cualquiera de los dos bandos opuestos podría acabar en la completa destrucción de ambos. La doctrina MAD suponía que cada bando poseía suficiente armamento para destruir a su oponente y que cualquiera de los bandos, de ser atacado por cualquier motivo por el bando opuesto, respondería al ataque con la misma fuerza o mayor. El resultado esperado era que la contienda escalara a un punto en que cada bando llegaba a la destrucción total del adversario. Esta doctrina suponía además que el armamento nuclear de los Estados se encontraba disperso por todo el mundo en diferentes tipos de plataformas, por lo que la idea de lanzar un primer ataque devastador sobre la totalidad del armamento atómico de un país para neutralizar un eventual contraataque igual de devastador, resultaba imposible.

Asumiendo que ninguno de los bandos sería lo suficientemente irracional como para arriesgar su propia destrucción, ninguno de ellos se atrevería a lanzar un primer

ataque, bajo el temor de la respuesta. Esta teoría condujo a una situación prolongada de paz tensa.

Norteamérica intentó, por medio de un proyecto presentado durante la Presidencia de Reagan, romper con los postulados de la teoría MAD a partir de la idea de poner en órbita terrestre sobre satélites y alojar en tierra un número determinado de plataformas espaciales artilladas con armamento láser y balístico. Este sistema, denominado BMD (*Ballistic Missile Defense*), consistía en un complejo sistema de sensores y ordenadores, cuyo cometido a grandes rasgos era el de detectar, identificar y hacer seguimiento a misiles en vuelo, que posteriormente serían destruidos por el armamento láser, lo que permitiría anular un ataque enemigo. El proyecto fue conocido popularmente como “guerra de las galaxias” y formaba parte de una iniciativa denominada Iniciativa de Defensa Estratégica (SDI) que, a diferencia de la MAD tenía un carácter defensivo. Aunque esta iniciativa nunca llegó a desarrollarse plenamente en la práctica, las investigaciones realizadas sirvieron para preparar el terreno a los posteriores sistemas antimisil de teatro.

Se pueden recordar algunos programas tecnológicos que fueron desarrollados en la década de los ochenta como el ERINT (*Extended Range Interceptor)* que formaba parte del Programa de Defensa de Misiles de Teatro y que era una ampliación del FLAGE (*Flexible Lightweight Agile Guided Experiment*) el cual desarrollaba la tecnología “dispara a matar” basada en un preciso y ligero sistema de guiado por radar. Estos sistemas experimentaron modernos sistemas propulsores de motor-cohete. Otros programas de la época fueron el HOE (*Homing Overlay Experiment*), el ERIS (*Exoatmospheric Reentry-vehicle Interceptio System*), el DEW (*Directed-energy Weapon*), y otros muchos que permitieron importantes avances en el empleo del láser, sensores, satélites, interceptadotes, contramedidas, sistemas de vigilancia y seguimiento y otros campos.

Independientemente de su valor estratégico, de las posibles vulnerabilidades del BMD, y de sus consecuencias en el orden mundial, lo que más interesante resulta a los efectos de este trabajo es que esta carrera armamentística supuso sin ningún género de dudas un importante impulso en lo referente a investigación y desarrollo tecnológico. A día de hoy se puede afirmar que, aunque la bomba atómica nunca fue utilizada después de Nagasaki, el mundo se benefició afortunadamente de aquel

equilibrio inestable y que supuso una auténtica revolución en la concepción de la guerra poniendo fin a lo que hasta entonces se entendía por “guerra total”.

Una nueva dinámica se ha establecido en el siglo XXI en lo concerniente al arma nuclear, desde que son las potencias regionales –y no sólo las globales- las que disponen o pueden disponer de dichas armas, cuando no determinados grupos o facciones con posibilidad de acceder, si no a la tecnología nuclear al menos a materiales radiactivos de desecho. De ellos hablaremos más adelante.

En este rápido y sucinto repaso a la evolución de la tecnología en las últimas siete décadas, es obligado dedicar unas líneas a las comunicaciones –medio que permite el ejercicio del mando dando soporte a la transmisión de órdenes hasta los escalones ejecutantes- y a la guerra electrónica, que como es sabido abarca todas las acciones encaminadas a asegurar el uso eficaz de las emisiones electromagnéticas propias e impedir que el enemigo pueda emplear las suyas.

El periodo de la guerra fría fue determinante en el progreso y evolución de la tecnología de las comunicaciones. Los más importantes avances fueron la comunicación satélite de órbita geoestacionaria, los sistemas de multiplexado y la transmisión de datos por conmutación de paquetes de información. A ellos se añadió la utilización de la fibra óptica en los años setenta, que permitía la utilización de un gran ancho de banda en redes fijas, con baja atenuación de la señal y gran seguridad en la comunicación.

En cuanto a las comunicaciones radio, durante esos años se desarrollaron de forma vertiginosa los sistemas de comunicaciones en todas las bandas, tanto en Frecuencia Modulada (FM) como en Amplitud Modulada (AM), consiguiéndose terminales cada vez más sofisticados, más potentes, menos pesados y más resistentes, que dotaban a las comunicaciones de rapidez, seguridad y fiabilidad.

En lo que respecta a la Guerra Electrónica (EW), que había nacido para abaratar lo costes y riesgos del espionaje convencional a principios del siglo XX durante la crisis italo-austriaca de 1908 y la guerra italo-turca del año 1911, se desarrolló exponencialmente el mismo día en que comenzó a funcionar el primer radar.

En el transcurso de la Segunda Guerra Mundial se experimentó por primera vez en combate y de forma continuada lo que los ingleses Wilkins y Rowe habían ideado unos años antes y que denominaron RADAR (*Radio Direction and Ranging*). Desde aquel momento la guerra electrónica no ha dejado de evolucionar al compás de la tecnología hasta constituirse hoy en día en un factor decisivo en el combate.

Tradicionalmente se ha dividido en tres áreas: Medidas de Apoyo de Guerra Electrónica (ESM), Contramedidas Electrónicas (ECM) y Medidas de Protección Electrónicas (EPM), también denominadas Contra-contramedidas electrónicas (ECCM). Este campo de la tecnología impregna la totalidad de las facetas del combate, puesto que abarca la aplicación de dispositivos integrados en sistemas aéreos, terrestres y marítimos para ser utilizados tanto en acciones ofensivas como defensivas, y cualquiera que sea el uso que se de al espectro electromagnético. Su evolución desde aquellos años del conflicto mundial ha sido constante hasta nuestros días y al compás de su progreso ha evolucionado la doctrina y la táctica.

Acciones como la búsqueda direccional de la emisión electromagnética encaminada a la localización o DF (*Direction Finding*), y el análisis del espectro con el fin de obtener información y evaluarla fueron utilizadas profusamente durante la Segunda Guerra Mundial y en conflictos posteriores.

A toda medida electrónica se opone la correspondiente contramedida y a ésta, a su vez, una nueva contracontramedida. De esta forma y a lo largo de las décadas que siguieron al conflicto mundial, se fueron desarrollando las tres grandes áreas de la EW.

A las primitivas técnicas empleadas por rudimentarios radiolocalizadores siguieron las de interferencia –tanto activa como pasiva- mediante perturbación o *jamming* o las de decepción o engaño, las cuales requerían nuevos equipos cada vez más sofisticados y capaces, que dieron lugar a las primeras ECM. El primero de los sistemas empleados para interferir fue el denominado *Window*, que era una rudimentario *chaff* a base de tiras de papel de estaño cuya finalidad era la de confundir mediante falsos ecos a los operadores de radar enemigos. En cuanto a la decepción, fueron las bengalas de infrarrojos los primeros artefactos que se utilizaron de forma sistemática para engañar a los radares enemigos.

Para eludir las contramedidas enemigas se fueron desarrollando como hemos dicho las correspondientes ECCM que consistían básicamente en desarrollar la capacidad de preservar los equipos propios de las perturbaciones enemigas. Así se desarrollaron tecnologías encaminadas a que los equipos pudieran “huir” de una frecuencia de trabajo con la rapidez suficiente para que ésta no fuera localizada por los equipos enemigos. De esta manera se empezó a desarrollar la tecnología de la *frecuency agility* que permitía cambiar rápidamente la frecuencia del equipo sin interrumpir la emisión y la de *frecuency diversity* que permitía operar en varias frecuencias.

La tecnología permitió también desarrollar el anulado de antena mediante la modificación de la ganancia de antena en determinadas direcciones, el ensanchamiento del espectro o la transmisión por ráfagas (*burst transmissión*).

Otras actividades llevadas a cabo en el marco de la EW en el periodo estudiado han sido las de recoger, evaluar, analizar, interpretar y valorar informaciones recogidas en el campo electromagnético, actividad conocida como Inteligencia de Señales (SIGINT) que se subdivide en Inteligencia de Comunicaciones (COMINT) cuando las señales proceden de las telecomunicaciones, e Inteligencia Electrónica (ELINT) cuando proceden de cualquier otra fuente.

No sólo las comunicaciones y el radar han sido actividades de guerra electrónica. También lo han sido el espectro infrarrojo, la electro-óptica y el láser.

De todos es sabido que desde que finalizó la estrategia de bloques a finales del siglo pasado, el orden mundial que nos ha tocado vivir se ha caracterizado por las denominadas amenazas asimétricas y omnidireccionales, que no precisan de la escalada nuclear de la que antes hablábamos para poner fin a la forma que tenemos de entender el mundo. Es más, incluso se recurre a formas tradicionales de destrucción o violencia que fueron utilizadas siglos atrás y que comparten espacio en el campo de batalla con las más modernas tecnologías. Podemos poner como ejemplo los gases utilizados en la guerra Irán-Irak, que en poco se diferenciaban de los de la Primera Guerra Mundial.

La guerra bajo formas no convencionales -como es el caso de la insurgencia, la guerrilla o el terrorismo- también son una muestra de la forma en que se pueden

utilizar métodos y tecnologías más propios del pasado, teniendo presentes por supuesto los numerosos matices que diferencian cada uno de los tipos de guerra mencionados. En muchos casos además, los grupos terroristas o insurgentes provistos de tecnologías no muy evolucionadas se enfrentan a naciones con alto nivel tecnológico cuyas Fuerzas Armadas están dotadas de armamento sofisticado. Son muchos los ejemplos históricos en que facciones irregulares han hecho frente con éxito a ejércitos dotados de avanzadas tecnologías. Podemos citar a la guerrilla del Vietcong frente a los norteamericanos, las derrotas de Francia en Indochina y Argelia, las de la Unión Soviética en Afganistán, o las de Israel en diferentes campañas en el Líbano frente a Hizbolá. Pero aunque sea la forma de hacer la guerra o el terreno, y no el número de misiles y su precisión, lo que constituya un factor clave para la victoria, eso no ha sido óbice a lo largo de la historia para que estos grupos hayan puesto todo su empeño en dotarse con modernos sistemas y armas. En concreto, a lo largo del siglo XX, los avances tecnológicos han permitido poner al alcance de estos grupos una serie de pequeños pero tremendamente poderosos artefactos, que van desde simples armas cortas a los más complejos misiles, pasando por modernos equipos de comunicaciones y todo tipo de explosivos.

En manos de los terroristas, la tecnología moderna ha convertido a la sociedad en mucho más vulnerable desde los años sesenta en que el terrorismo internacional comenzó a tomar auge. Un simple misil antiaéreo puede derribar un avión con cientos de pasajeros civiles y un escape de gas tóxico en el metro de una gran ciudad puede producir cientos de bajas y aterrorizar a todo un continente.

Desde los años noventa en que el arsenal nuclear soviético quedó en buena medida fuera de control, se ha barajado la posibilidad –no sin cierto tremendismo- de que los grupos terroristas puedan hacerse con la tecnología necesaria para fabricar una bomba atómica. Aunque esto sería prácticamente inviable, no se descarta el uso de un explosivo convencional para diseminar material radiactivo sobre un área de terreno con el fin de producir daños a las personas o dejar la zona inhabitable. Este tipo de técnica, más accesible a los terroristas que las armas nucleares por su diseño más sencillo, constituyen las denominadas “bombas sucias”, que aunque usan elementos radiactivos no desencadenan reacción nuclear alguna. Tampoco se

puede descartar el empleo por estos grupos de determinados componentes biológicos o químicos.

Es preciso añadir que en la lucha contra el terrorismo, la más avanzada tecnología no siempre ha sido capaz de distinguir al terrorista de su entorno, y las más sofisticadas armas no han podido discriminarlo de quienes le rodean, por lo que los ataque quirúrgicos no han sido posibles y lo daños colaterales han sido inevitables, con el correspondiente tributo de cara a la opinión pública.

Para algunos autores, la llamada guerra asimétrica se produjo como reacción a una nueva teoría nacida en Estados Unidos denominada “Revolución en los Asuntos Militares”. Sólo mediante este tipo de guerra se podía hacer frente a la desproporcionada ventaja tecnológica de Estados Unidos, puesta de manifiesto en la segunda guerra del Golfo y posteriormente en Serbia-Montenegro. Esta RMA (*Revolution in Military Affaires*) no es otra cosa que una teoría sobre el futuro de la guerra, generalmente relacionada con la tecnología y los aspectos organizativos, ligada de forma particular a la tecnología de la información, las comunicaciones y la tecnología espacial, y cuyo objetivo es permitir recomendaciones en el campo de la defensa relativas a la transformación de las Fuerzas Armadas y a la plena integración de sistemas. Aunque muchos países han intentado en los últimos años llevar a cabo esta RMA, sólo han podido iniciar los procesos correspondientes aquellos que estuvieron dispuestos a hacer fuertes inversiones en ella.

Este orden mundial que antes hemos dibujado, ha dado paso a la era de la información, en la que cobran especial importancia desde el punto de vista tecnológico los sistemas de información, que permiten al mando contar con la información necesaria para dominar al adversario, entre los que se encuentran los Sistemas C4I, (*Command Control, Communications, Computer and Information*), las redes digitales los sistemas de posicionamiento global. De ellos hablaremos en capítulos posteriores.

Para finalizar podríamos hacer algunas reflexiones que nos permitan resumir las ideas expresadas y obtener algunas conclusiones:

- La historia reciente demuestra que, en ocasiones, ha sido la tecnología la que ha hecho evolucionar los conceptos del arte de la guerra y, en otros momentos, ha

sido la tecnología la que ha tenido que avanzar para estar a la altura de los requerimientos operacionales. Aunque los avances tecnológicos hayan propiciado cambios en la forma de conducir la guerra, no parece que hayan influido –en sentido estricto- en las causas de los conflictos, independientemente del interés que puedan tener los fabricantes de armamento en vender sus productos. Sin embargo, no faltan quienes defienden una teoría determinística según la cual el momento propicio para iniciar una guerra, sobre todo si ésta era inevitable, venía marcado por la oportunidad del momento tecnológico que vivían sus ejércitos.

- Permaneciendo fijos el resto de los factores, cuanto menos complicado es el escenario en que se lleva a cabo el combate, mayores son las ventajas que proporciona la alta tecnología.

- En las últimas décadas, cada desarrollo tecnológico en el campo de la defensa se ha visto seguido por el correspondiente desarrollo para combatirlo o neutralizarlo, de manera que cada generación de armas está permanentemente expuesta a quedar obsoleta y ser superada o mejorada por otra más efectiva.

- La historia reciente demuestra que en la mayoría de los ámbitos de la guerra, ningún arma es suficiente por sí sola.

- Uno de los legados de la Segunda Guerra Mundial ha sido la confianza que ha despertado la tecnología tanto en el ámbito militar como en el civil. Es un hecho comprobado –naturalmente con las correspondientes salvedades- que la tecnología militar en diferentes países y regiones tiende a homogeneizarse por efecto de la globalización: los materiales y equipos que resultan eficaces para un determinado país o ejército, son adquiridos rápidamente por otros. Esta uniformidad lleva en muchos casos a generar también réplicas similares en la conducción de la guerra, en los procedimientos, tácticas y doctrinas.

- La maniobra con movimientos rápidos de evasión y la dispersión de las unidades en los ámbitos de la guerra terrestre naval y aérea fue una consecuencia de los avances en la precisión y potencia de las armas. El resultado fue el aumento de problemas para batir el blanco y en la comunicación de unidades entre sí y de estas con sus puestos de mando y control. Para hacer frente a estos problemas, se dedicó un gran esfuerzo a la investigación y desarrollo en el campo de la

electrónica para asegurar la transmisión el ejercicio del mando y la coordinación, esto es, para hacer las comunicaciones seguras, flexibles y fiables.

- Posiblemente la dedicación a la electrónica ha hecho que los avances en otros campos hayan quedado en un segundo plano o se hayan realizado a un ritmo más lento, de manera que desde la Segunda Guerra Mundial apenas se hayan percibido sustanciales o revolucionarios cambios. Tales podrían ser los casos de los motores de combustión interna o determinados sistemas de amortiguación de vehículos, por poner algún ejemplo.

- Ningún país puede permitirse retirar las viejas armas o sistemas en uso sin antes disponer de su correspondiente reemplazo. Por otro lado, el impulso tecnológico que supone la constante investigación y el desarrollo de nuevas armas, es el responsable de que en las últimas décadas se multiplicara el número de modelos diferentes de armas y sistemas simultáneamente en servicio. Por tal motivo, y con la idea permanente de obtener la máxima eficacia de todos ellos, se produjo una imparable tendencia a la integración, que a su vez hizo que se diera la paradoja de que siendo cada elemento por separado menos valioso, unos y otro fueran interdependientes.

- La mayoría de los sistemas de armas han sido diseñados para enfrentarse a otras máquinas, no para hacerlo a personas.

La tecnología permitirá en un futuro muy próximo encriptar la información de manera que las comunicaciones sean inviolables. Si se codifica la información en átomos, dicha información puede ser estructurada en forma de luz, enviarla a otro grupo de átomos, e imprimir desde ellos la información. Es lo que se denomina comunicación cuántica, que sin duda encontrará pronto su aplicación militar. Pero eso ya pertenece al futuro.

Bibliografía

- ÁLVAREZ, Cristóbal “A Summarized History of the Development of Military Technology”. www.warscholar.com
- ARCANGELIS, Mario de. Historia de la guerra electrónica. Editorial San Martín. Madrid, 1983.

- BALARAM, P. “Science, Technology and War”. Current Science. Nº 7, Vol 84, abril 2003.
- BARKER, A.J. La Guerra del Yom Kippur. Editorial San Martín. Madrid, 1975.
- BUZAN, Barry. Introducción a los Estudios Estratégicos. Tecnología Militar y Relaciones Internacionales. Ediciones Ejército. Madrid, 1991.
- GRAY, Colin S. How Has War Changed Since the End of the Cold War. Discussion Paper. National Intelligence Council.
- HOWARD, Michael, & GUILMARTIN, John F. “Two Historians in Technology and War”. www.au.af.mil
- JARYMOWYCZ, Roman. “The History of Military Technology”. Précis EO 400.1. www.cfsj. Forces.gc.ca/oic/
- MARTÍ SEMPERE, Carlos. Tecnología de la Defensa. Instituto Universitario “General Gutiérrez Mellado” (UNED). Madrid, 2006.
- PARKER, Geoffrey (ed.). The Cambridge History of Warfare. Cambridge University Press. Ohio 2005.
- RIDLER, Jason S. “Thinking Outside the Black Box: Some Historical Inquiries into the Relationship of Technology and Warfare”. War Studies of the Royal Military College of Canada. www..cda-cdai.ca
- ROLAND, Alex. “Technology and War”. American Diplomacy. www.unc.edu
- TOWNSHEND, Charles. The Oxford History of Modern War. Oxford University Press. New York 2000.
- VAN CREVELD, Martin. Tecnology and War. The Free Press. New York, 1991.
- _____ Modern Conventional Warfare: An Overview. Discussion Paper. National Intelligence Council.
- WRIGHT, Quincy. A Study of War. The University of Chicago Press. Midway Reprint. Chicago, 1983.

CAPÍTULO SEGUNDO

LAS FUERZAS ARMADAS ESPAÑOLAS Y LAS NUEVAS TECNOLOGÍAS EN LA ERA DE LA INFORMACIÓN, SITUACIÓN ACTUAL

LAS FUERZAS ARMADAS ESPAÑOLAS Y LAS NUEVAS TECNOLOGÍAS EN LA ERA DE LA INFORMACIÓN. SITUACIÓN ACTUAL

Por ENRIQUE HERRERA CORTÉS

Introducción

El Diccionario de la Lengua Española nos define “tecnología” como:

> “Conjunto de los conocimientos propios de un oficio mecánico o arte industrial.// 2. Tratado de los términos técnicos.// 3. Lenguaje propio de una ciencia o arte // 4. Conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto”.

El número de tecnologías que se enmarcan en esta definición es muy amplio, de ahí la necesidad de definir unos criterios de clasificación y una jerarquía en la que encuadrar las tecnologías de interés para la defensa. En este sentido, el Plan Director de Investigación y Desarrollo (PDID) nos dice:

> “Las tecnologías de interés militar son aquellas que contribuyen a que las Fuerzas Armadas se doten con los sistemas de armas y equipos lo más avanzados que sea posible para cumplir sus misiones.”

Asimismo, identifica una taxonomía de referencia “taxonomía tecnológica del PDID”.que distingue dos grandes grupos de tecnologías: tipo A y tipo B.

Las tecnologías tipo A, denominadas “subyacentes” o “capacitadoras”, son tecnologías de carácter más básico o multisectorial que sirven de fundamento a las tecnologías orientadas a sistemas de defensa. Se trata de tecnologías duales en las que el Investigación y Desarrollo (I+D) está liderado por el sector civil. Se estructuran en dos niveles: área y tecnología, con un total de 11 áreas y 81 tecnologías. Las 11 áreas “subyacentes” son:

- A01 Materiales estructurales y análisis de efectos estructurales.

- A02 Materiales relacionados con la firma y materiales para estructuras inteligentes.
- A03 Materiales electrónicos.
- A04 Materiales y dispositivos fotónicos/ópticos.
- A05 Dispositivos electrónicos y eléctricos.
- A06 Tecnologías para materiales energéticos y plasma.
- A07 Materiales químicos y biológicos.
- A08 Tecnologías informáticas.
- A09 Proceso de señal y tratamiento de la información.
- A10 Ciencias humanas.
- A11 Tecnologías del entorno físico.

Las tecnologías tipo B “orientadas a sistemas” son aquellas tecnologías que de manera directa facilitan el diseño, la fabricación y las pruebas de sistemas de armas y equipos. Abarcan un total de 141 tecnologías, agrupadas bajo 34 subáreas y 16 áreas. Estas áreas son:

- B01 Letalidad.
- B02 Protección de plataformas.
- B03 Propulsión.
- B04 Generación de energía y combustibles.
- B05 Plataformas.
- B06 Armas.
- B07 Guerra electrónica y armas de energía dirigida.
- B08 Sistemas sensores, control y reducción de firma.

- B09 Sistemas de guiado, presentación, proceso y control.
- B10 Simuladores, entrenadores y entornos sintéticos.
- B11 Integración de sistemas.
- B12 Tecnologías de comunicación.
- B13 Tecnologías CIS.
- B14 Tecnologías del combatiente.
- B15.Técnicas y herramientas de diseño ensayos, experimentación y procesos de fabricación.
- B16 Técnicas de Infraestructura y medio ambiente.

Las tecnologías tipo B son las que presentan un mayor interés desde el punto de vista de la defensa y por lo tanto las que se van a tener en consideración en el estudio. Estás tecnologías están continuamente vigiladas, para conocer su evolución y asegurarse de que cuando tengan que ser utilizadas por las Fuerzas Armadas se empleen de la forma más eficaz y eficiente posible. De ello son responsables los observatorios tecnológicos, que constituyen el Sistema de Observación y Prospectiva Tecnológica, órgano de asesoramiento creado por la Dirección General de Armamento y Material (DGAM).

Áreas tecnológicas

Letalidad

El objetivo fundamental en este área siempre ha sido disponer de tecnología para las cabezas de guerra y penetradores con la finalidad de obtener municiones más eficaces, más seguras y al menor coste posible, teniendo en cuenta su ciclo de vida.

Las tecnologías que actualmente se utilizan en España en relación con las cabezas de guerra son las siguientes:

- La tecnología por colado en munición convencional, que es la más extendida en bombas de aviación y proyectiles de artillería, está basada en el trinitrotolueno

(TNT) como único componente o como ligante energético de otras sustancias explosivas (hexogeno para obtener Hexolita, octógeno para Octolita, aluminio para Tritonal). En algunos países se está cambiando la carga de TNT por otro explosivo que proporciona a la munición menor sensibilidad a los estímulos externos:

- La tecnología de explosivos de naturaleza plástica (PBX) colados, que es comparable a la utilizada por los países de nuestro entorno.

- Las tecnologías de prensado para explosivos (prensado de simple acción, prensado de doble acción y prensas con platos calientes) son dominadas por la industria nacional.

- La tecnología para la obtención de los sistemas de armado. La tecnología de estos sistemas es dominada por la industria nacional. El problema surge cuando hay que utilizar explosivo PBX, de una gran insensibilidad, para ello se está utilizando el detonador de impacto *slapper* del que tenemos cierta experiencia y disponemos de la capacidad suficiente para su fabricación.

- Los elementos pirotécnicos (detonadores, multiplicadores, retardos, etc.) se encuentran totalmente desarrollados por la industria nacional.

- Tecnologías específicas de espoletas electrónicas utilizadas en diversos tipos de armas para mejorar las prestaciones de las cabezas de guerra y dotarlas de mayor seguridad y fiabilidad. En España las espoletas electrónicas que han sido desarrolladas y puestas en servicio por las Fuerzas Armadas han sido básicamente de funcionamiento al impacto o con tiempo de retardo y se han realizado avances importantes en las espoletas opto electrónicas, por lo que las necesidades están cubiertas y la tecnología está al nivel de los países de nuestro entorno.

- Tecnología de revestimientos Liner ([6]) para el cono metálico que recubre el explosivo de la cabeza de carga hueca. Actualmente se está aplicando esta

[6] Es una lámina metálica curva, que sufre un complejo proceso de deformación para convertirse en el proyectil a partir de la explosión.

tecnología a materiales de altas densidades (níquel, molibdeno, wolframio y tantalio), estando la industria española capacitada para realizarlos.

- La tecnología Follow-Through es una tecnología combinada, de cargas huecas y penetradores, que se aplica principalmente a bombas o dispensadores aire-tierra de penetración y que, para un mismo peso de la carga, duplica la capacidad de penetración. La industria española está en condiciones de desarrollar esta tecnología.

- Tecnologías para optimizar la preparación de nuevos materiales energéticos, que tienen una baja sensibilidad y mantienen una alta energía, mediante materias primas comerciales de bajo coste. Estos nuevos materiales no están comercializados y para disponer de ellos es necesario sintetizarlos. Con este objetivo, el Laboratorio Químico Central de Armamento (LQCA) ha puesto en marcha un laboratorio de síntesis con material y personal formado al efecto.

En relación con los penetradores, los proyectiles perforantes por energía cinética, de calibre igual al del arma que los dispara, han sido totalmente sustituidos por proyectiles subcalibrados (munición flecha). Estos proyectiles subcalibrados alcanzan mayores prestaciones y son capaces de perforar los blindajes compuestos, reactivos o no, gracias a la alta velocidad con que son disparados. España dispone de la tecnología necesaria para fabricar este tipo de munición.

Protección de plataformas

La protección de las plataformas sigue siendo un elemento importante para asegurar la supremacía en el campo de batalla, considerando la protección, directa e indirecta de la plataforma, no como un elemento añadido, sino formando parte de la estructura resistente del vehículo. La pugna tradicional entre el proyectil y la coraza, desnivelada hacia uno u otro lado a lo largo de la Historia, sigue estando presente como motor del desarrollo militar.

La protección directa para vehículos terrestres, basada en “blindajes activos”, está suficientemente desarrollada en la industria española, que tiene capacidad para el diseño, desarrollo, producción y pruebas de este tipo de sistemas de protección, y dispone de los materiales necesarios para su fabricación. Sin embargo, para la

protección directa basada en “blindajes pasivos” hay una fuerte dependencia exterior en relación con la producción de los materiales empleados (aleaciones de titanio, cerámicos avanzados y fibras avanzadas).

En relación con la protección directa de las plataformas navales que, independientemente de donde proceda la amenaza, dependen de: la compartimentación del buque, la utilización de determinados tipos de materiales, el empleo de refuerzos estructurales y de determinados grosores de plancha (blindaje). En cuanto a la compartimentación del buque, no se dispone de ningún programa para el análisis de su vulnerabilidad. La contratación es exterior, por no considerarse rentable el desarrollo de un programa para realizar este tipo de análisis. Para la elección del espesor del material de blindaje, que da la protección conjuntamente con la plancha de acero del buque, se dispone de información de la Organización del Tratado del Atlántico Norte (OTAN) y especificaciones militares. Asimismo, los equipos que se montan en los buques de guerra deben probarse al choque, según la norma MIL-S-901-D ([7]), para ello estos equipos se montan sobre tacos elásticos homologados cuya tecnología es conocida por nuestra industria.

La protección directa de plataformas aéreas consiste básicamente en la utilización de paneles de blindaje en las zonas críticas de dichas plataformas y más concretamente en la cabina de la tripulación. Estos paneles, fabricados en Kevlar y compuestos cerámicos, van unidos a los compartimentos y asientos de la tripulación mediante *fasteners* que permiten la fácil retirada del mismo cuando el tipo de misión no requiera esta protección. Para la tecnología de estos paneles es aplicable lo comentado anteriormente para los vehículos terrestres.

La protección indirecta para vehículos terrestres está basada en diferentes artificios (ocultación, señalización, iluminantes, incendiarios, señuelos, etc.), en los que somos autosuficientes y son fabricados por la Fábrica Nacional de la Marañosa (FNM).

---

[7] Norma que recoge las especificaciones militares sobre la resistencia a los impactos ocasionados por el choque del buque.

La protección indirecta para plataformas navales concibe a la plataforma como una defensa espacial y en profundidad en las que de una forma secuencial y automatizada se llevan a cabo las siguientes acciones: evitar la detección por el enemigo; detectar, localizar y mantener el seguimiento de la amenaza; clasificar la amenaza y alertar de su presencia y evitar el impacto. Para cada una de estas acciones se adoptan distintas medidas como: empleo de técnicas *stealth* ([8]), reducción de firmas, sistemas de apantallamiento, sensores y señuelos. Estas tecnologías serán estudiadas en otros apartados del capítulo.

En relación con la protección indirecta de las aeronaves, en esta área vamos a considerar solamente los señuelos en sus diferentes tipos (chaff y bengalas). La tecnología que se utiliza para producir estos señuelos se encuentra disponible en la industria nacional.

Propulsión

Para el estudio del área tecnológica de sistemas de propulsión vamos a considerar las tecnologías siguientes:

- Turbina de gas.
- Motores alternativos y rotativos de combustión interna.
- Propulsión eléctrica rotativa.
- Transmisión y elementos cinemáticos finales.
- Motores cohete. Propulsante sólido.
- Motores cohete híbridos.
- Estatorreactores.
- Propulsión en tubos armas.

[8] Técnicas que se utilizan para control y reducción de firma.

La turbina de gas sigue siendo crucial en la propulsión de plataformas militares aéreas, sin tener sustituto a corto plazo, y desempeñando asimismo un importante papel en la propulsión de plataformas militares navales y terrestres. Para tener la turbina de gas es necesario disponer de la correspondiente tecnología de diseño de componentes, de definición de sistemas, de materiales, de procesos de fabricación, de integración y de ensayos. En este sentido, en España la dependencia del exterior es fuerte, a excepción de las dos últimas tecnologías citadas, pero incluso en éstas estamos supeditados al suministro de piezas y repuestos.

Salvo raras excepciones, todas las plataformas militares, terrestres y navales, son equipadas con máquinas de combustión interna, desarrolladas y fabricadas expresamente para esta finalidad, y basadas en el motor de ciclo diesel. En general, todos los desarrollos tratan de concentrar el máximo de potencia en las mínimas dimensiones y peso. En la actualidad, salvo la serie de motores Bravo, desarrollada por Navantia (antigua Bazán) junto con Caterpillar, el resto de motores utilizados en aplicaciones militares son fabricados con licencia de tecnologías extranjeras y algunos elementos importantes de estos motores son adquiridos en el exterior.

Dentro del apartado de propulsión eléctrica rotativa se consideran aquellos equipos que, accionados por una máquina de combustión interna, generan energía eléctrica aplicable a la propulsión de buques o vehículos. La tecnología relacionada con la propulsión eléctrica rotativa es de fabricación extranjera, contando con la industria nacional solamente para los generadores de corriente continua y corriente alterna.

Los componentes que transmiten la potencia desde el motor hasta el elemento final (elemento cinemático) que genera el empuje para el movimiento, son diferentes dependiendo del tipo de plataforma, teniendo cada tipo una transmisión y un elemento cinemático característicos. En las plataformas aéreas y marítimas son las hélices y en plataformas terrestres las ruedas, cadenas, etc. Actualmente, no existe en España capacidad de desarrollo de un sistema de transmisión completo para una plataforma aérea y la dependencia exterior es prácticamente total. Solamente existe capacidad de participación en el desarrollo de algunos elementos integrantes del sistema de transmisión (sistemas de lubricación) o capacidad de fabricación de componentes del sistema ya diseñado.

Los sistemas de propulsión para cohetes se basan en propulsantes sólidos con cargas de una forma geométrica determinada, en función de la misión. En España se ha realizado un gran esfuerzo en esta área y hay una serie de organismos y empresas, el LQCA, el Instituto Nacional de Técnica Aeroespacial (INTA), etc., con capacidad para desarrollar y fabricar los componentes y subsistemas correspondientes, por lo que las necesidades militares actuales pueden ser perfectamente cubiertas por la industria española.

El interés por los motores cohete híbridos, como sistema de propulsión, aumenta debido a las ventajas inherentes a dichos motores frente a los motores cohete de propulsante líquido, incorporando sus tecnologías. A nivel europeo varias instituciones, entre las que cabe citar al INTA, han trabajado juntos, con un contrato de la Agencia Europea del Espacio, en la investigación de las aplicaciones de este tipo de motores. En lo relativo al diseño conceptual del sistema, la dependencia del exterior puede considerarse prácticamente nula, pero es elevada a la hora de proceder al desarrollo real de un motor cohete híbrido, especialmente al referirnos a la disponibilidad de las materias primas para la fabricación del bloque de combustible sólido y de los materiales termoestructurales habitualmente utilizados en el desarrollo de los sistemas de propulsión para estos motores.

Los aerorreactores representan una tecnología madura que se está proponiendo como sistema de propulsión de la próxima generación de misiles. Podemos clasificarlos como estatorreactores (*ramjet*), estatocohetes (*ramrocket*) y estatorreactores de combustión supersónica. Actualmente, debido a la gran cantidad de tecnologías involucradas en un dispositivo Ramjet (aerodinámica, tomas dinámicas, sistema de combustión, estructura, combustible, motor de aceleración, dispositivos de detección y guiado, etc.), sería complicado abordar un sistema completo por parte de la industria española, sin embargo es importante significar que el LQCA dispone de una instalación experimental, desarrollada conjuntamente con la Escuela Técnica Superior de Ingenieros Aeronáuticos (ETSI Aeronáuticos), para pruebas de motores tipo estatocohete y estatorreactor de propulsante sólido. La línea de investigación que se sigue en el LQCA pretende desarrollar todas las tecnologías del estatorreactor (*ramjet*) y del estatocohete (*ramrocket*), por lo que es posible obtener sus tecnologías básicas.

La propulsión en tubos armas incluye toda la gama de cañones convencionales, eléctricos y los de propulsante líquido. Los cañones son, y seguirán siendo en el futuro, ampliamente utilizados. Todos ellos responden al concepto clásico y utilizan tecnologías semejantes. Esto no quiere decir que esta tecnología esté estancada, ya que continuas mejoras han llevado a una clara superioridad de unos sistemas frente a otros. Estas mejoras se han centrado en la aplicación de nuevos materiales para disminuir peso; en la mejora de los diseños de los proyectiles, permitiendo obtener mejores alcances y eficacias, disminuir la vulnerabilidad del sistema ante un impacto; disminuir las posibilidades de detección y obtener mejoras en la balística de las cargas propulsoras. La tendencia principal es la que pretende disminuir la vulnerabilidad de las municiones ante impactos externos y de este modo disminuir también la vulnerabilidad de las plataformas. En este sentido, España participa en un programa internacional sobre “pólvoras de baja vulnerabilidad LOVA”. La consecuencia principal, en relación a la tecnología de la vulnerabilidad de las municiones, será que nuestra dependencia exterior, cuando finalice este programa internacional, se limitará a alguna de las materias primas. Por otra parte, aunque en España se perdieron capacidades importantes como consecuencia de la casi nula inversión de los años noventa, el desarrollo del cañón de 155 milímetros para el Ejército de Tierra, que es el primer sistema de artillería completo que se fabrica después de un lapso de tiempo de casi 40 años, unido a la adquisición de la tecnología de fabricación del cañón de 120 milímetros del *Leopardo E 2*, han supuesto un impulso tecnológico importante.

Generación de energía y combustibles

El conocimiento actual de las fuentes energéticas y su potencialidad de uso para la explotación es muy preciso. Ello incluye los mecanismos de conversión de energía y el desarrollo tecnológico que se requiere para llevarlos a la práctica.

En relación con los generadores eléctricos en buques, la industria auxiliar española está perfectamente capacitada para el suministro de las plantas eléctricas que sean necesarias, cumpliendo con las especificaciones de choque, vibraciones y ruido que se determinen, incluida la normativa de contaminación ambiental. Por lo que se refiere a los generadores eléctricos en aeronaves, aunque la tecnología de cualquier sistema de generación de potencia eléctrica está bastante madura, todos

los elementos de los sistemas eléctricos son fabricados por tecnología extranjera por lo que la dependencia del exterior es completa. En cuanto a los microgeneradores eléctricos que incorpora la munición hay que señalar que las tecnologías implicadas en los dispositivos, fundamentalmente electromecánicas, son clásicas y accesibles para la industria española.

Las aplicaciones militares de las baterías son muy variadas, tales como la tracción de vehículos (submarinos), arranque de motores (carros de combate y aeronaves), alimentación de equipos electrónicos espaciales, de emergencia, transmisores y señalización, misiles y munición. La posición de la industria española de baterías eléctricas, es relativamente aceptable, pues la producción de baterías para submarinos y carros de combate es nacional, pero en las baterías de armamento, aeronaves y equipos electrónicos (litio, plata-cinc), se depende totalmente del exterior. Los sistemas eléctricos o electrónicos que incorpora la munición, ya sea para el guiado de ésta (detectores, circuitería de proceso y actuadores en misiles) o para la detección de blancos e iniciación de la cabeza de guerra (sensores y circuitos de proceso y disparo en espoletas) requieren fuentes de energía eléctrica embarcada y segura. En los casos donde no es posible obtener energía eléctrica a partir de los diversos parámetros dinámicos presentes en el entorno balístico, la fuente empleada es una batería capaz de generar energía mediante un proceso electroquímico. Los principales tipos de baterías que actualmente se emplean son las de formación y las térmicas. España dispone de industrias con acceso a las tecnologías implicadas en estos dispositivos, pero lo específico de las aplicaciones unido al reducido volumen de la demanda hace que existan muy pocos fabricantes en el mundo, siendo todos ellos extranjeros. Esta circunstancia, unida al hecho de que la mayoría de los fabricantes son a la vez responsables del sistema que las incorpora, determina que la dependencia exterior sea absoluta.

Las aplicaciones Eléctricas de Radiofrecuencia (RF) son muy variadas, por lo general están ligadas a las comunicaciones y a las señales electromagnéticas, si bien tienen un importantísimo campo de uso en los aceleradores de partículas, que es donde se encuentran las fuentes de RF de mayor potencia. Actualmente existen dos grandes familias de dispositivos para este tipo de aplicaciones: tubos de vacío y de estado sólido y aunque la madurez industrial internacional de este sector es muy sólida está dominada por los países más avanzados. En España no existe ningún

acelerador de porte alto o medio, y la industria nacional para la fabricación de estas fuentes es de tamaño reducido.

En relación con los generadores de potencia acústica, si se exceptúan las instalaciones de megafonía sobradamente conocidas, que usan el aire como medio de transmisión y que son fabricadas en prácticamente todas las naciones, el resto de los dispositivos, (corredereras acústicas, sondadores, sistemas de detección usando sonoboyas, balizas, teléfonos submarinos, contramedidas acústicas, productores de ruido, torpedos activos y sonares) usan el agua de mar como medio de transmisión. La industria nacional no dispone de las tecnologías aplicadas a los dispositivos que usan el agua como medio de transmisión, aunque están desarrolladas por otros países.

Las pilas de combustible son una familia de tecnologías que utilizan distintos electrólitos, elemento que determina su clasificación y que operan a diferentes temperaturas. Con carácter general puede decirse que, para aplicaciones militares, la naturaleza silenciosa de las pilas de combustible y la baja firma de infrarrojo de las de baja temperatura son sus características más significativas. En la mayoría de los casos, el combustible y su almacenamiento son los principales problemas para la penetración de esta tecnología. Para la fabricación de *stack* (módulo de células apiladas) dependemos totalmente del exterior. Sin embargo, la ingeniería del reformado del combustible y la conversión de corriente continua a alterna es fácilmente abordable por diversas compañías españolas.

La tecnología de combustibles y lubricantes son conocimientos maduros que sufren procesos de aceleración periódicos a medida que los sectores tecnológicos asociados, es decir vehículos y motorizaciones, se desarrollan. A su vez, esos sectores asociados son impulsados por factores tecnológicos (los nuevos materiales, la computerización de los sensores y las exigencias medio ambientales). Puesto que la tendencia generalizada es que las motorizaciones militares sean cada vez más similares a las civiles, no parece adecuado el desarrollo generalizado de combustibles y lubricantes específicos de uso militar, con la excepción de aquéllos para determinados sistemas de armas. Las industrias presentes en el mercado español están en una posición tecnológica que podemos calificar de suficiente para afrontar los cambios a corto plazo.

Plataformas

La industria naval española, tanto civil como militar, tiene un gran peso específico en el concierto internacional, disponiendo de grandes astilleros así como centros de investigación. Navantia, que desde hace 50 años es el contratista principal de nuestra Armada, ha construido la practica totalidad de nuestras unidades, tanto de superficie como submarinas .El ejemplo más significativo son las fragatas clase F100. Además, España cuenta con el Canal de Experiencias Hidrodinámicas de El Pardo (CEHIPAR), con instalaciones adecuadas para la experimentación fiable con modelos físicos. El CEHIPAR posee unos laboratorios y canales perfectamente preparados y equipados para desarrollar una amplia gama de investigaciones en este campo, y con una amplia experiencia en el campo de la Mecánica de Fluidos Computacional (CFD). Podemos decir que el binomio Navantia-CEHIPAR es perfectamente competitivo frente al exterior en el campo del diseño hidrodinámico de buques y cuenta con los conocimientos y los medios necesarios para realizar los proyectos de los buques que necesite nuestra Armada.

El factor movilidad y su repercusión en la supervivencia de las plataformas móviles terrestres, sometidas a diferentes agentes (terreno, tiempo de exposición, etc.), focalizan la atención prioritaria de requerimientos operativos para estas plataformas. La situación actual de la movilidad, en lo que se refiere a vehículos blindados, no es la que se contempla como necesaria para el futuro. Se requiere pues el estudio de un nuevo vehículo que reemplace al actual y que deberá disponer de los últimos adelantos en materia de suspensiones interactivas. Esto no es problema para la industria española que cuenta con gran parte del capital humano que desarrolló la suspensión del Vehículo Blindado sobre Ruedas (BMR) y la del vehículo de combate de Infantería (VCI *Pizarro*).

En relación con las aeronaves, las guerras recientes (guerras del Golfo, Bosnia, Kosovo, Afganistán) han vuelto a demostrar la importancia de la superioridad aérea, que necesita de aeronaves muy ágiles con altas prestaciones en misiles y radar. Al mismo tiempo, la disminución de los presupuestos de Defensa obligan a disponer de aeronaves multimisión, y multifunción siendo requisitos clave la capacidad de penetraciones con mayor alcance y gran agilidad o bien, una agilidad determinada con mayor tiempo de combate. En el futuro todos los aviones de combate avanzados

estarán basados en la tecnología llamada de empuje vectorizado. Esta tecnología es el elemento clave para facilitar a los aviones de caza el sobrevivir en un combate aéreo y la superioridad en los combates dentro y fuera del alcance visual del enemigo. En este sentido la Industria de Turbo Propulsores S.A. (ITP) ha desarrollado una tobera vectorial, basada en patentes españolas, que hace previsible que la industria española sea líder en este sector. Por otra parte, la experiencia obtenida por la compañía EADS-CASA ([9]) en el desarrollo y la producción del *Eurofighter* (EF-2000), junto con su fusión con la compañía alemana DASA (*Daimler Chrysler Aerospace*) permiten prever un puesto relevante para la industria aeronáutica española.

En relación con las plataformas de entrenamiento, exponer que la introducción en España de modernos sistemas de armas tales como el F-18 y el EF-2000 ha implicado la necesidad de un entrenamiento avanzado de pilotos sobre plataformas con unas características muy específicas. El desarrollo del EF-2000 ha significado un importante salto cualitativo y cuantitativo en el proceso de adquisición de tecnología y ha contribuido decisivamente al posicionamiento industrial español en el sector aeronáutico europeo.

En lo referente a Vehículos Aéreos no Tripulados (UAV), el INTA tiene desarrollado un sistema completo de vigilancia electroóptica por medio de estos vehículos, de uso civil y militar, aunque la dependencia exterior es muy grande. No obstante, como en el desarrollo de los UAV las tecnologías aerodinámicas y estructurales utilizadas son muy parecidas a las utilizadas en el resto de las aeronaves, la base tecnológica existente en la industria española en las áreas de navegación, control, guiado y transmisión de datos, así como en las de gestión de vuelo y misión, permitiría abordar los desarrollos indicados con un riesgo técnico aceptable.

El panorama español, en relación con las plataformas espaciales, ha experimentado un notable cambio en las dos últimas décadas donde las industrias españolas están desarrollando productos espaciales de alto valor añadido, aunque en gran medida estos productos están orientados hacia un entorno de aplicaciones civiles. El INTA

[9] European Aeronautic Defense and Space Company – Construcciones Aeronáuticas S.A.

posee una serie de laboratorios de I+D con gran capacitación técnica en casi todas las áreas tecnológicas implicadas en el sector. Por otra parte, en el Programa de Pequeños Satélites (MINISAT 01, CESAR, ISHTAR, MINISAT 21, etc.), se ha adquirido experiencia tanto en la gestión como en la ingeniería de sistemas de programas espaciales. El INTA cuenta con una serie de instalaciones para integración y ensayos de vehículos espaciales donde se llevan a cabo programas de pequeños satélites. También, aunque a una escala mucho menor, hay que citar ciertos institutos del Consejo Superior de Investigaciones Científicas (CSIC) y a las universidades. Así pues, aunque todavía el sector espacial nacional no tiene el tamaño crítico necesario para poder abordar en su totalidad el desarrollo de un satélite de tamaño medio, como puede ser un satélite de comunicaciones comercial, sí se dispone de la capacidad tecnológica precisa para llevar a cabo proyectos de menor envergadura.

Armas

La situación actual es compleja por la diversidad de armas que, con la misma finalidad, utilizan nuestras Fuerzas Armadas, teniendo ello escasa justificación técnica, pues se encarece la adquisición y el mantenimiento, y limita la participación de las empresas españolas en su diseño, desarrollo y suministro.

Para realizar el estudio vamos a agrupar los diferentes tipos de armas en los siguientes grupos:

- Cohetes, cohetes de dispersión reducida y lanzacohetes.
- Portadores de submunición.
- Armas ligeras.
- Armas antiblindados.
- Obuses.
- Armas antimisil.
- Armas antitorpedo.

– Bombas guiadas.

Las armas del grupo de cohetes, en dotación en las Fuerzas Armadas, están obsoletas o tienen su vida útil excedida. Aunque en este campo, el LQCA está trabajando en un demostrador tecnológico, cuyo objetivo final es disponer de un cohete de dispersión reducida con capacidad para portar municiones inteligentes con cabezas de guerra tipo EFP ([10]). Dentro del mismo programa se están estudiando mejoras en los lanzadores en línea para: disminución de peso, protección de sirvientes, automatización de operaciones, etc.

La situación actual de las armas portadoras de submunición se reduce a las bombas cluster que tiene de dotación el Ejército del Aire. Otros desarrollos, en grado diferente de avance, son las cabezas dispersoras del cohete Teruel (con munición bivalente contra carro y contra personal), las minas contra carro y la munición de mortero MAT-120 ([11]) (portadora de granadas anticarro y antipersonal).

En relación con las armas ligeras, aunque han evolucionado muy poco durante los últimos decenios, la industria española tiene una gran experiencia en este campo habiendo diseñado y fabricado distintos tipos de fusiles y ametralladoras. Los conceptos de fusil de asalto y la ametralladora de apoyo siguen siendo empleados en la actualidad de forma similar a como se empleaban hace 35 años. La evolución de las armas de Infantería se ha reducido a la incorporación de materiales más modernos (plásticos), mejoras de los materiales tradicionales y a la incorporación de sistemas de visión. Puede decirse que la única innovación significativa es el lanzagranadas automático de 40 milímetros, que está desplazando progresivamente a las ametralladoras medias y pesadas, debido a su gran potencia de fuego y a su capacidad de saturación de zona.

En el grupo de armas antiblindados dos son los procedimientos utilizados para el ataque a este tipo de vehículos: proyectil de carga hueca o similar y proyectil de energía cinética. Entre los medios del primer tipo, disponibles en la actualidad, nos

---

[10] (Explosively Formed Proyectiles). También conocidos por SFF (Self Forged Fragment) y Misznay Schardin. En ocasiones, la P de la sigla se refiere a Penetrator, la F a Forged.

[11] Munición de 120 mm, de tipo “cargo”, que transporta 21 submuniciones y cada una de ellas produce efectos tanto de penetración como de fragmentación.

encontramos con el material C90 ([12]) para una defensa próxima hasta 300 metros y con el *Alcotan 100* ([13]) para una defensa a mayor alcance (hasta 500 – 600 metros). La industria española en la munición correspondiente a sistemas contracarro de carga hueca presenta un nivel medio competitivo. El campo de la munición de energía cinética ya fue tratado en el apartado letalidad.

La Artillería de Campaña (ACA) ha llevado a cabo un proceso de renovación con la incorporación del obús de 105 milímetros *lightgun*, los nuevos obuses de 155 milímetros o la modernización de las Baterías Autopropulsadas (ATP). La modularidad de los diseños permite añadir *kits* que incorporan, entre otros: sistemas de navegación inercial, computadores balísticos o su integración en redes computerizadas de mando y control de fuego. Esto va a posibilitar que la renovación acometida mantenga su validez en los próximos años. Asimismo, la industria nacional, alentada por el proceso de renovación de materiales, debe tomar posiciones que le permitan, a medio plazo, mantener un nivel tecnológico equiparable al resto de los países de nuestro entorno.

En la actualidad las armas antimisil son, en su mayoría, evoluciones de la artillería antiaérea clásica y podemos agruparlas en:

- Cañones multitubos (*Vulcan Phalanx*, *Samos, Meroka*, etc.).
- Sistemas misil antimisil. (*Crotale*, *Ram*, etc.).
- Sistemas de señuelos. (*Dagaie*,*Barricade*,etc.)

El único desarrollo de la industria española ha sido el arma multitubo *Meroka* naval. Actualmente es posible abordar, con recursos nacionales, la modernización de este sistema de armas y colaborar en la actualización de sistemas similares que fueran de interés para las Fuerzas Armadas. Asimismo, se está en condiciones de desarrollar un afuste terrestre que soporte el *Meroka* naval. En relación con los sistemas misil antimisil y de señuelos, nuestro país no tiene conocimiento suficiente

[12] Lanzagranadas contracarro que, dependiendo del modelo, utiliza distintas municiones.

[13] Sistema de arma que bate distintos objetivos con distintas municiones: antitanque, antibunker y antimaterial (doble propósito)

para abordar su desarrollo a medio plazo, a no ser que se decida iniciar el despegue tecnológico en esta materia con la colaboración de las empresas extranjeras de nuestro entorno que ya lo poseen. En todo caso, el grado de dependencia exterior es elevado, en lo que se refiere al material electrónico *y* materias primas básicas para la elaboración de componentes.

En relación con las armas antitorpedo, podemos decir que actualmente las formas de combatir la amenaza submarina se centran en sistemas perturbadores acústicos, remolcados por el propio buque. La industria española no ha participado en los desarrollos de los sistemas actuales, por lo que la dependencia exterior es total.

Las bombas de guiado están siendo uno de los elementos más utilizados en los últimos conflictos en los que se han visto envueltas las fuerzas de la OTAN (Irak, Bosnia, Kosovo y Afganistán). La ausencia de una fuerza aérea enemiga de interceptación ha hecho que la única amenaza sea la defensa antiaérea de baja cota (artillería, misiles SAM, etc.), lo que ha motivado cambios tácticos, evitando en lo posible los vuelos a baja cota y realizando lanzamientos desde alta cota. Por otro lado, en los conflictos actuales se pretende minimizar no sólo las bajas propias, sino evitar en la medida de lo posible los daños colaterales, lo que exige la mejora de precisión frente a las bombas convencionales. No existe actualmente ningún sistema de bomba guiada de desarrollo español en servicio, aunque hay empresas capaces de fabricarlas si reciben apoyo para el diseño y desarrollo de algunos subsistemas.

Guerra Electrónica (EW) y armas de energía dirigida

El empleo masivo de las tecnologías con base en la microelectrónica para el control, dirección y mando de los sistemas de combate, ha convertido a la EW en un campo en constante evolución, que debe responder a los cambios continuos de unas amenazas que también se aprovechan del rápido desarrollo de las mismas tecnologías. De hecho, los recientes conflictos avalan el principio militar, aceptado desde hace décadas, de que la victoria, en cualquier futuro conflicto, será del que controle el espectro electromagnético.

Según el tipo de tecnología empleado en sus sensores los diferentes equipos de EW se clasifican en: electroópticos, de radiofrecuencia, magnéticos, eléctricos y acústicos. La utilización de esta tipología se justifica porque las características

operativas de los equipos (precisión, alcance, tamaño, peso y coste) están muy condicionadas por su pertenencia a cada grupo. Sin embargo, las diferencias tecnológicas las determina el subsistema sensor ya que el resto de los sistemas comparten las mismas técnicas y tecnologías de procesado de señal y datos, integración, etc.

Las naciones, entre ellas España, han tratado hasta el momento de permanecer lo más independientes posible en el desarrollo de Sistemas EW. Esta situación, en el caso de las naciones europeas, tiende a cambiar, por motivos fundamentalmente presupuestarios, y se vislumbra un planteamiento de I+D, dentro de un entorno europeo, en el que los grandes consorcios serán la norma y en los que debe estar la industria nacional.

Actualmente, la industria nacional en sistemas de EW de comunicaciones, frente a otros suministradores internacionales, presenta graves deficiencias. Podemos decir que a nivel de componentes de proceso y en una gran mayoría de subconjuntos se depende completamente del exterior.

En relación con los Sistemas de EW radar, la empresa INDRA Sistemas ha conseguido una capacidad industrial con niveles similares a otras industrias del mundo, sobre todo en el ámbito naval (sistema Aldebarán) ([14]) y aéreo (Sistema Dass) ([15]), por lo que el grado de madurez de la tecnología en la industria nacional y la dependencia respecto a los suministradores externos, se restringe principalmente a la adquisición de componentes para la fabricación de sistemas.

Para los sistemas acústicos, utilizados únicamente en unidades de la Armada, la dependencia exterior es absoluta.

En lo que se refiere a los Sistemas IR/visible/UV ([16]), las tecnologías empleadas por la industria nacional, en los señuelos de infrarrojos (IR) de protección de plataformas aéreas y buques, son capaces de generar cortinas de ocultación sólo para la región

[14] Sistema de Defensa electrónica utilizado por la Armada Española y marinas de otros países

[15] Sistema de auto-defensa electrónico utilizado por el Ejército del Aire y realizado por INDRA en consorcio con otras empresas europeas.

[16] Tres regiones del espectro electromagnético, Infrarroja, Visible y Ultravioleta.

del espectro visible e infrarrojo cercano (VNIR), no habiéndose desarrollado ningún artificio con características multiespectrales. La dependencia exterior en relación con perturbadores activos capaces de interferir en el proceso de adquisición, seguimiento y guiado de misiles y armas inteligentes dotadas de buscadores IR, es absoluta. Otro tanto cabe decir de las tecnologías de los Sistemas de Energía Dirigida (láseres, microondas de alta potencia y armas de haces de partículas cargadas).

Sistemas sensores, control y reducción de firma

Actualmente, la integración y trabajo combinado de múltiples y diferentes sensores (activos y pasivos) permite operar en periodos prolongados, en condiciones todo tiempo y en ambientes de contramedidas y de saturación electromagnética. Asimismo, para mantener la superioridad militar, es fundamental disponer de sensores cada vez más sofisticados y de los medios necesarios para reducir al máximo su detectabilidad. Estos sensores necesitan de una gran diversidad de tecnologías para las que la industria nacional tiene diferente capacidad de respuesta. En líneas generales podemos decir que la industria nacional dispone de capacidades en determinadas subáreas tecnológicas, donde trata de ser competitiva, e intenta adquirir tecnología en aquellas subáreas en las que se dispone de menores capacidades, con aportaciones de terceros países.

Las tecnologías en las que, existe mayor potencialidad, bien por existir un mayor conocimiento, o por haber industrias capacitadas con interés en desarrollarlas, son las siguientes:

- Sensores y antenas activas y pasivas de radiofrecuencia.
- Sensores de ondas milimétricas y micromilimétricas activos y pasivos.
- Sensores láser, IR, visibles y UV.
- Control y reducción de firmas radar y de ondas milimétricas y micromilimétricas.
- Control y reducción de firmas IR, visibles y UV.

Las tecnologías en las que existe una cierta potencialidad y se tiene un gran interés por disponer de ellas son:

- Sensores químicos.
- Sensores de explosivos.
- Sensores inerciales.
- Control y reducción de firmas láser.

En relación con el control y reducción de firma, la tecnología *stealth* utilizada es multidisciplinar y necesita conjugar distintas áreas tales como diseño, aerodinámica, materiales, medidas y cálculo electromagnético, utilizando potentes computadores. Estas tecnologías son aplicables a todas las plataformas para reducir su vulnerabilidad, por lo tanto de gran interés para las Fuerzas Armadas. En España se es consciente de la importancia de que los sistemas de armas posean firmas bajas frente a todos los sensores utilizables y se están haciendo grandes esfuerzos para adquirir un nivel tecnológico que nos permita ser menos dependientes.

En los temas de control y reducción de la firma Radar hemos realizado algunos progresos y podemos decir que: disponemos de métodos de cálculo electromagnético y modelización; se realiza investigación de materiales absorbentes al radar (RAM) y se está participando en programas y proyectos europeos. No obstante, la dependencia exterior es elevada sobre todo en la realización de ensayos y en la disponibilidad de materiales y pinturas RAM. Referente al control y reducción de firmas IR/UV/Visible, láser, magnéticas y acústicas, el retraso es aún mayor que en la firma Radar, aunque se debe significar que el INTA, FNM y el LQCA han realizado trabajos de determinación de firma IR/UV/Visible. En cuanto al control y reducción de firmas eléctricas y electromagnéticas podemos decir que la empresa española Saes Gamesa es una de las pocas compañías en el mundo que disponen de la tecnología adecuada y probada para los sensores eléctricos.

Sistemas de guiado, presentación, proceso y control

Las tecnologías de guiado y control están jugado un papel fundamental en la mejora de la precisión de las armas, lo cual tiene dos implicaciones inmediatas: por un parte

el ahorro económico, al necesitar menor número de proyectiles para neutralizar un blanco, y por otra un aumento de la moral de las tropas propias, al comprobar que se dispone de un armamento eficaz que produce grandes efectos sobre el enemigo y muy pocas bajas en el bando propio, por lo que su empleo, en los ejércitos modernos, va creciendo en cada conflicto bélico.

Para el estudio de esta área vamos a tener en cuenta las tecnologías utilizadas en los siguientes sistemas:

- Navegación y guiado.
- Control y estabilización.
- *Hardware.*
- *Software.*
- Interfaz hombre-máquina

Las tecnologías usadas para los sistemas de Navegación y Guiado dependen enormemente de los sensores en los que se basan. Se ha alcanzado un alto grado de desarrollo en muchos de ellos, pero el progreso previsible en ciencias como la óptica o la física de estado sólido, entre otras, nos auguran una evolución muy significativa en los próximos años. Las tecnologías utilizadas por estos sistemas son: inercial, radioeléctrica por satélite, doppler, ayudas radioeléctricas desde tierra, ondas milimétricas, autoguiado con radar de microondas, teleguiado, sonido, etc. La situación actual, excepto en ayudas radioeléctricas desde tierra y teleguiado, es de una gran dependencia exterior, que es mayor si nos referimos a componentes.

En los Sistemas de Control y Estabilización la industria española ha tenido relativamente poca demanda para la realización de sistemas de control aeroespaciales, esto no quiere decir que no esté capacitada para afrontar programas avanzados de investigación y desarrollo. En el campo de las aplicaciones navales, la industria nacional dispone de las capacidades necesarias para el diseño e implementación de sistemas integrados de control de buques. En el campo de control del tiro se dispone de la capacidad necesaria para el desarrollo y fabricación de direcciones de tiro terrestres y navales, para todo tipo de artillería, utilizando

sensores de seguimiento activos (radar, telémetros láser) y/o pasivos (seguidores automáticos de vídeo con imágenes del espectro visible o infrarrojo).

En relación con el *hardware*, la industria nacional ha desarrollado un procesador digital de señal de altas prestaciones, para radares militares tridimensionales, de largo alcance. También ha desarrollado un sistema de control que permite la gestión de los elementos que constituyen un sistema complejo, por medio de redes de área local y con capacidad para conectarse con redes externas. En resumen, podemos decir que la industria nacional tiene capacidad suficiente para el diseño y fabricación de tarjetas procesadoras de propósito general, que necesitan la mayoría de los sistemas actuales, pero existe una dependencia total en cuanto a componentes básicos: microprocesadores y memorias.

En cuanto al *software*, dado que el mercado civil se ha convertido en el motor de desarrollo de tecnologías para estos sistemas, el sector militar, cada vez más, se comporta como un usuario de estos desarrollos, adaptando, en la medida de lo posible, los productos comerciales a sus requisitos. La industria española posee, por lo general, un alto grado de capacidad en el diseño/desarrollo de *software*. Esta capacidad es diferente dependiendo del tipo de *software* (base, aplicación) utilizado. Para el *software* de base se suele utilizar el diseñado y desarrollado por el fabricante (sistemas operativos, controladores, etc.), sin embargo, para el software de aplicación se tiende a ser independientes y diseñar/desarrollar soluciones propias (EF-2000, F-18, etc.).

Por último, en relación con los componentes, *hardware* y *software*, que tienen por objetivo seleccionar o generar información, presentarla a los usuarios del sistema y permitir su interacción (interfaz hombre-máquina), podemos decir que la industria nacional tiene capacidad tecnológica suficiente para desarrollar este sistema, aunque en el *hardware* utilizado, como ya se apuntó anteriormente, hay una gran dependencia a nivel de componentes básicos: microprocesadores y memorias.

Simuladores, entrenadores y entornos sintéticos

La necesidad de los Sistemas de Simulación ha sido sentida en las Fuerzas Armadas desde hace muchos años, aunque fue a partir de la década de los noventa cuando se avanzó mucho en la mentalización de todos los escalones de mando

sobre la necesidad de la simulación para conseguir un adecuado nivel de adiestramiento con un coste ajustado.

Los campos que se van ha considerar, en relación con los Sistemas de Simulación, son los siguientes:

- Ayudas a la enseñanza, instrucción y adiestramiento.
- Campos de tiro y maniobra instrumentalizados y simuladores de campo.
- Blancos simulados.
- Entrenadores y simuladores de misión (simuladores tácticos).
- Juegos de guerra.

Como ayudas a la enseñanza, instrucción y adiestramiento, actualmente, las maquetas y elementos inertes constituyen una importante área de aplicación de las técnicas básicas de la simulación. Los sistemas multimedia, en sus diferentes niveles (vídeos, programas interactivos, etc.), también están incluidos en este tipo de ayudas. En este campo somos autosuficientes.

De los diferentes modos de empleo de los campos de tiro: fuego real, puntería con fuego simulado y combate entre unidades, es en los dos últimos donde la simulación tiene su aplicación. La utilización de estos modos de empleo nos permite reducir considerablemente el entrenamiento con fuego real. En la actualidad se dispone de diferentes sistemas de simuladores tácticos de combate, de una y doble vía, pero con una servidumbre importante, no son compatibles y por lo tanto no pueden ser interoperables. Esta falta de integración reduce sensiblemente las capacidades de operación de tales sistemas. La versión aérea de los campos de tiro instrumentalizados la constituyen los Sistemas ACMI ([17]) que permiten el empleo de aviones reales en maniobras de combate con determinación en tiempo real de los efectos del fuego simulado.

[17] (Air Combat Maneuvering Instrumentation) es un sistema implementado en aviones de combate para analizar el vuelo en tres dimensiones y poder estudiar las maniobras realizadas.

Tradicionalmente los blancos simulados, para las prácticas de fuego real o simulado, se basan en la presentación de una diana con diferentes apariencias y aspectos. Generalmente, el blanco lleva algún tipo de sensor que permite determinar, con un elevado grado de precisión, el impacto del proyectil y sistemas de control para el reposicionamiento de los blancos y su presentación de forma variable en el tiempo. Un caso especial de blancos simulados son los simuladores de escenarios, para la práctica de tiro con armas ligeras. El Ejército de Tierra dispone de este tipo de blancos simulados. Por otra parte, también pueden ser considerados blancos simulados todos los sistemas de presentación de blancos, radar y sonar, empleados en la Armada y en Ejercito del Aire. La Armada dispone de un simulador que reproduce el sistema de combate de las fragatas y del portaaeronaves *Príncipe de Asturias*. Igualmente, el Ejército del Aire y la flotilla de aeronaves de la Armada disponen de un simulador para el entrenamiento de controladores aéreos.

En la actualidad las Fuerzas Armadas disponen de un amplio conjunto de entrenadores, simuladores y juegos de guerra que cubren gran parte de sus necesidades. Estos sistemas se mejoran periódicamente con la adaptación de las nuevas tecnologías que van irrumpiendo en el mercado, como la interconexión vía HLA ([18]) entre simuladores.

Por último decir que, en el diseño, desarrollo y producción de sistemas de entrenamiento basados en la simulación, la industria española presenta un alto grado de madurez, dando muestras en innumerables ocasiones de su capacidad para la concepción, desarrollo y producción de los sistemas, partiendo de los requisitos operacionales, incluso para mercados exteriores, como es el caso del AV8Bplus para las Armadas norteamericana e italiana. Sin embargo, hay que significar la fuerte dependencia de la industria española al nivel de componentes para: sistemas de presentación de imagen, plataformas de movimiento, generadores de imagen, etc.

Integración de sistemas

[18] (High Level Architecture) es la arquitectura técnica de referencia para la interoperabilidad entre simuladores.

Los costes derivados de problemas de integración (económicos, temporales, funcionales e incluso humanos) pueden superar, en los sistemas de cierto nivel de complejidad, a los costes de desarrollo de los propios subsistemas. Esto nos lleva a pensar que la Integración de Sistemas (IS) es un área a tener muy en cuenta y es necesario vigilar su evolución. Para su estudio la vamos a desglosar en las subáreas siguientes:

- Ingeniería de sistemas.

- Diseño y desarrollo integrado.

En general, la complejidad de los sistemas actuales va en aumento, con la aparición de nuevas tecnologías, en un entorno que cambia sin cesar. Esto, unido a la falta de un método disciplinado para la obtención de nuevos sistemas, ha provocado, en numerosas ocasiones, que los resultados hayan sido excesivamente costosos por no haber definido adecuadamente los requisitos al inicio del proceso, por no haber efectuado el necesario análisis para evaluar los riesgos asociados con las decisiones adoptadas en las primeras fases, y por no haber adoptado un procedimiento metódico y estructurado en el diseño y desarrollo de los sistemas. El problema se está corrigiendo y actualmente podemos decir que, por parte del ministerio de Defensa, se presta especial atención a la integración de los sistemas ya existentes con aquellos que se están adquiriendo o se prevé adquirir en el futuro.

Desde la perspectiva del diseño y desarrollo integrados cabe decir que la capacidad de la IS para desarrollar sistemas complejos, con la funcionalidad necesaria, en coste y plazo adecuados, pasa a través de la utilización de tecnologías de integración. Es por ello que este tipo de tecnologías son críticas para los sistemas militares, pues permiten flujos de información más simples, predecibles y explotables, que facilitan el desarrollo de sistemas complejos.

La dependencia exterior de esta área tecnológica es nula, pues en España hay suficiente conocimiento en estas disciplinas y no es necesaria la participación de técnicos o empresas extranjeras para su desarrollo. Las carencias de esta área provienen más de una utilización inadecuada de los conocimientos disponibles que de la necesidad de importar conocimiento de otros países. No obstante, es necesario coordinar su desarrollo en España con el de los países aliados, sobre

todo, teniendo en cuenta las perspectivas futuras de concentración de la industria de defensa y los posibles proyectos internacionales.

Actualmente el ministerio de Defensa cuenta con una empresa pública, Ingeniería de Sistemas para la Defensa de España S. A. (ISDEFE), creada específicamente para prestar servicios de consultoría y asistencia técnica en ingeniería de sistemas y tecnologías avanzadas a organismos y empresas del sector público, con especial dedicación al propio Ministerio.

Tecnologías de comunicación

El área de tecnologías de comunicación comprende las tecnologías necesarias para comunicar o transmitir información de diversa naturaleza (voz, datos, texto, gráficos, imágenes y vídeo) de un punto a otro, mediante diversos tipos de medios (aire, agua, cable o fibra) y formas (electromagnéticas, acústicas, y luminosas), y todo ello con la confidencialidad adecuada. Para su estudio se ha tenido en cuenta la siguiente división:

- Transmisión/Recepción:
  - Comunicaciones de RF.
  - Comunicaciones láser.
  - Comunicaciones acústicas.
  - Redes y servicios de comunicación.
- Seguridad de las Comunicaciones:
  - Criptología.

En relación con las tecnologías utilizadas en los equipos de comunicación RF la dependencia exterior es total, a excepción de algún equipo en la banda de UHF ([19]), en los que la industria nacional está participando en consorcios internacionales encargados de su desarrollo y fabricación. En cuanto a las tecnologías de

[19] (Ultra High Frequency) Frecuencia Ultra Alta.

comunicaciones de microondas y ondas milimétricas, que principalmente utilizan bandas de frecuencias destinadas a las comunicaciones vía satélite, la dependencia en repetidores embarcados y elementos de la plataforma de los satélites es elevada. En estaciones de comunicaciones la dependencia exterior se limita a componentes y prácticamente somos autosuficientes en el campo de la integración, fabricación, apoyo logístico de equipos y sistemas y en el equipamiento auxiliar.

En las tecnologías de comunicaciones láser, acústicas y redes y servicios de comunicación tenemos una dependencia exterior absoluta, aunque el número de fabricantes y su distribución mundial aseguran la disponibilidad de los dispositivos necesarios.

El conjunto de tecnologías que proporcionan confidencialidad, autenticidad e integridad a las comunicaciones conforman la criptología. Aunque en este campo hemos evolucionado mucho, es necesario seguir incidiendo en la necesidad de crear una “conciencia de seguridad” que aún queda en evidencia, por sus deficiencias, cuando tomamos parte en proyectos supranacionales con países de nuestro entorno. Actualmente, los sistemas criptológicos que se utilizan en el ministerio de Defensa, que son certificados por el Centro Criptológico Nacional perteneciente al Centro Nacional de Información (CNI), en su gran mayoría son sistemas de fabricación nacional.

Tecnologías CIS

Los Sistemas de Comunicaciones y de Información (CIS) están conformados por un conjunto de equipos, métodos, procedimientos y personal organizados para realizar las funciones de transferencia y proceso de la información. Actualmente las tecnologías que utilizan, aun siendo muy diversas, tienen en común los siguientes aspectos:

- Están en continua evolución, quedando obsoletas en periodos de tiempo del orden de dos/tres años.

- El mercado está liderado por las aplicaciones civiles y cada vez es menos recomendable el desarrollo específico de tecnologías militares.

- Se apoyan cada vez más en tecnologías comerciales (COTS) y cuando no existen estos productos se apoyan en productos desarrollados para uso en más de una aplicación (NOTS y GOTS).

- Cada vez es más importante el intercambio de información entre sistemas homogéneos o heterogéneos, dependientes de una organización o dependiendo de organizaciones dispersas.

Asimismo, el desarrollo de estos sistemas está muy condicionado por nuestra pertenencia a organismos internacionales -Organización del Tratado del Atlántico Norte (OTAN), Organización de Naciones Unidas (ONU), etc.- y los compromisos adquiridos. Para su estudio vamos a tener en cuenta lo división siguiente:

- Diseño Integrado de CIS.

- Normativa para la interoperabilidad de los CIS.

- Técnicas de seguridad de los CIS.

- Identificación de plataformas no cooperadoras.

- Fusión de datos y de información.

- Digitalización del campo de batalla.

- Ayudas a la decisión.

En relación con el diseño integrado de CIS los sistemas nacionales que actualmente existen en las Fuerzas Armadas han seleccionado, por lo general, productos comerciales de infraestructuras muy similares, y en línea con las recomendaciones OTAN. Al mismo tiempo, han proliferado en el mercado los productos comerciales de conectividad, por lo que la interoperabilidad técnica es un problema relativamente resoluble, aunque no así la interoperabilidad funcional y operativa, que es un problema mucho más complejo y más difícil de resolver. En general, los sistemas no trabajan de forma integrada y no disponen, en muchos casos, de comunicación

física de datos entre ellos, aunque en Euromids ([20]) se están dando pasos para resolver este problema. En cuanto al diseño de estructuras de datos, existe una gran variedad de modelos propios, y derivados de diferentes trabajos de grupos OTAN, que son incompatibles entre sí. Esto dificulta fuertemente la integración de los sistemas nacionales, reflejando un problema que existe en el entorno OTAN y que sólo se prevé resolver de forma satisfactoria a largo plazo. En este caso, el volumen y complejidad del desarrollo de *software* a realizar, a pesar de la potencia de las herramientas disponibles, supone la principal limitación para la cobertura y alcance de los sistemas actuales. De las tecnologías de la información relacionadas, tanto en *hardware* como en *software*, se puede afirmar, en términos generales, que la industria española no tiene desarrollos ni productos propios. Las empresas españolas se limitan normalmente a realizar la integración, instalación y mantenimiento de equipos/productos/sistemas fabricados en el exterior.

Actualmente es necesario disponer de una normativa de interoperabilidad CIS para que nuestras Fuerzas Armadas puedan integrarse en contingentes multinacionales y operar con ellos. En este sentido, en España se sigue la pauta marcada por la OTAN y se aplica de manera general el programa de interoperabilidad de la Alianza. Por otro lado se están utilizando conexiones entre las simulaciones y los sistemas CIS como ayuda al entrenamiento conjunto y como sustitución o complemento a los ejercicios con fuerzas reales. En España los Sistemas de Modelización y Simulación (M&S), y los Sistemas de Mando Control Comunicaciones Computadores e Inteligencia (C-4I), generalmente se han diseñado de manera estanca, sin tener en cuenta una posible interoperatividad entre ellos. En las tecnologías necesarias para estos sistemas hay una dependencia muy elevada del exterior, principalmente en software básico.

En relación con la identificación de plataformas no cooperativas, España ha participado en diferentes proyectos que en general han tenido un carácter de I+D. Los últimos conflictos nos han permitido sacar conclusiones sobre importantes carencias en identificación de blancos terrestres no cooperativos en un entorno rural y la necesidad de asistencia automática para la identificación de blancos en tiempo

[20] Consorcio europeo formado por las industrias de Francia, Alemania, Italia y España que participan

real. La resolución de estos dos puntos está imprimiendo un nuevo ímpetu al desarrollo en este campo en los países OTAN, entre ellos España, y ha generado nuevos proyectos de Identificación Automática de Blancos (ATR), casi todos ellos centrados en la tecnología radar en tres dimensiones (3D). En el campo de la Identificación cooperativa España está participando en diversos proyectos como el IFF modo 5 ([21]).

En España, la fusión de datos y de Información está muy condicionada por los requisitos que a nuestras Fuerzas Armadas se le imponen por su pertenencia a la OTAN y por la posibilidad de tener que llevar a cabo distintas acciones dentro de la Alianza. Asimismo, la fusión de datos y de información está supeditada a las funcionalidades requeridas en los centros de toma de decisiones y a los medios empleados. En cuanto a la situación tecnológica, la participación de empresas españolas en consorcios europeos, como el avión de combate europeo (EFA) ha permitido establecer la colaboración con países de nuestro entorno.

Conceptualmente, la digitalización del campo de batalla consiste en la aplicación de las tecnologías de la información para la adquisición, intercambio y empleo de la información a lo largo del campo/espacio de batalla, adaptada a las necesidades de los distintos componentes humanos del mismo. En la época actual, de presupuestos reducidos y de simplificación de la estructura de la fuerza, la digitalización del campo de batalla se percibe como el factor multiplicador de la fuerza más eficaz para garantizar la victoria en un mínimo tiempo y con el menor número de bajas propias.

En nuestras Fuerzas Armadas existen distintos programas de adquisición de Sistemas de Mando y Control para cada uno de los tres ejércitos que incorporan funcionalidades y tecnologías similares, aunque no existe una acción de coordinación en cuanto a los procesos funcionales a implementar y las tecnologías básicas a emplear.

En España la ayuda a la toma de decisiones está dando sus primeros pasos. La necesidad de este tipo de funcionalidad queda patente a raíz del lanzamiento de una

---

en el programa Multifuntional Information Distribution System (MIDS).

[21] Sistema de Identificación, Amigo – Enemigo utilizado por los países OTAN.

serie de iniciativas, como el Programa EUCLID ([22]), realizadas por los países del entorno de la Unión Europea Occidental, que España está obligada y todavía a tiempo de seguir para no perder el tren de la evolución tecnológica en este tema. Así mismo, el Laboratorio de Ensayos del Centro de Investigación y Desarrollo de la Armada (CIDA) en colaboración con la empresa española Sener Ingeniería y Sistemas S. A., ha desarrollado un prototipo de sistema de ayuda a la decisión para la identificación naval.

Tecnologías del combatiente

Desde la perspectiva del campo de batalla completo no se puede considerar la adquisición de equipos para el soldado de manera parcial, tales como armas individuales, cascos, máscaras, etc., sino que hay que considerar al soldado como un todo, es decir, como un sistema, siendo fundamental tener en cuenta las soluciones que aportan los avances tecnológicos a los problemas actuales.

De los estudios realizados sobre este tema se concluye que el combatiente tiene una serie de carencias y limitaciones que es posible mejorar apoyándose en las tecnologías actuales. El conjunto de estas mejoras constituye lo que se ha denominado "Combatiente futuro de Infantería Ligera/Mecanizada de primera Generación" (CIL-1G), objetivo del Programa de I+D "Combatiente futuro" que actualmente hay en las Fuerzas Armadas. Las tecnologías fundamentales implicadas en este combatiente futuro de primera generación son:

- Tecnologías de ingeniería de sistemas.
- Tecnologías de armamento.
- Tecnologías de protección balística y otros.
- Tecnologías de protección nuclear, biológica y químicas y otras.
- Tecnologías de la fisiología del combatiente.

[22] Programa de Investigación y Tecnología promovido por los países del antiguo Grupo de Armamento de Europa Occidental (GAEO) con el objetivo de fortalecer la cooperación industrial, tecnológica y científica en el Sector Europeo de la Defensa.

- Tecnologías del vestuario.
- Tecnologías de sensores.
- Tecnologías de la información.
- Tecnologías de dispositivos de entrada/salida.
- Tecnologías de mando y control.
- Tecnologías de simulación.

El nivel tecnológico actual en España para hacer frente al desarrollo de estas tecnologías, excepto en tecnologías del vestuario, nuclear, biológica y química y simulación, es bajo o nulo, dependiendo mayoritariamente de la industria extranjera. Aunque es importante significar los esfuerzos que están realizando algunas empresas españolas, junto con diferentes Ministerios de Defensa y del Interior de países OTAN, desarrollando Programas I+D, para conseguir algunas de estas tecnologías.

Técnicas y herramientas de diseño ensayos,

experimentación y procesos de fabricación

Para su estudio parece conveniente desglosar esta área en las subáreas siguientes:

- Técnicas y herramientas de diseño.
- Técnicas de ensayos y experimentación.
- Técnicas y herramientas para procesos de fabricación.

Las técnicas encaminadas a reducir el ciclo de diseño constituyen un objetivo importante a alcanzar por la industria, pues su consecución está íntimamente relacionada con el coste final del producto. En relación con las tecnologías mecánicas básicas hay una gran dispersión de aplicaciones aunque la mayoría de las herramientas genéricas de diseño, potencialmente aplicables al mundo militar, están aplicadas en el mundo civil. Actualmente, el desarrollo de herramientas y técnicas en España, que sean competitivas frente a las de otros países, es fruto de

esfuerzos aislados sin una organización y cohesión interna clara. Se da el caso paradójico que, universidades, institutos, y empresas tienen colaboraciones mas estrechas con instituciones en el extranjero que nacionales. Una racionalización de esta situación seria un paso adelante muy importante pues se esta perdiendo una oportunidad histórica para hacer progresos de primera magnitud en este campo.

En cuanto a las técnicas y herramientas de diseño electrónico, el esfuerzo de las empresas españolas del sector de defensa para adaptar sus departamentos de diseño a los nuevos métodos es notable, pues hay que tener en cuenta que las series de fabricación son muy cortas y por lo tanto la formación de personal como la selección y adquisición de herramientas EDA ([23]) e Ingeniería Concurrente (IC) tienen un elevado coste. En cuanto al desarrollo de herramientas EDA, la dependencia del exterior es absoluta. En relación con la IC, se están llevando a cabo programas europeos de desarrollo e implantación de esta metodología con participación española.

En relación con las técnicas de ensayos y experimentación se hacen las siguientes valoraciones:

- Para los ensayos de cohetes y misiles, el LQCA está en disposición de poder realizar pruebas de vigilancia, de homologación o el desarrollo de líneas de I+D.

- En el campo de ensayos químicos la industria nacional se encuentra en buena posición pero con dos importantes limitaciones, la baja implantación de este tipo de material en nuestras Fuerzas Armadas y la falta de centros especializados.

- En España existen una serie de centros, INTA y Centro Logístico de Armamento y Experimentación (CLAEX), y la empresa EADS-CASA que tienen sus propios departamentos de ensayos en vuelo de aeronaves.

- La industria española tiene capacidad para realizar la mayor parte de los ensayos de componentes de vehículos terrestres y posee una capacidad baja en ensayos acreditados de movilidad de vehículos militares. La carencia mayor se manifiesta

[23] (Electronic Design Automation) Automatización del Diseño Electrónico.

en la falta de normas que definan el patrón de referencia de las magnitudes a medir.

- La industria española está aumentando su capacidad en el sector de los ensayos aerodinámicos pero la dependencia exterior sigue siendo importante.

- En la realización de los ensayos de optrónica, la industria española es muy deficitaria. No existen laboratorios independientes que puedan realizar los ensayos requeridos ni que incorporen un sistema de calidad adecuado y reconocido internacionalmente.

- Aunque hay centros y empresas que poseen tecnología para los ensayos ambientales, mecánicos y climáticos, actualmente las capacidades tecnológicas de los equipos han sido rebasadas por las necesidades.

- En relación con los ensayos radiológicos, en España no hay experiencia ni instalaciones para ensayos de tipo nuclear. Se dispone de laboratorios de medidas de radiaciones ionizantes, principalmente dedicados a medidas medioambientales y control de equipos utilizados en las instalaciones nucleares, radioactivas y médicas de uso civil.

La necesidad en la industria de obtener elevadas cotas de productividad con los menores costes posibles, para así poder competir, se hace extensiva a todos los productos que puedan ser adquiridos por Defensa. Estas características, unidas a las de fiabilidad, determinan el interés de potenciar las técnicas y herramientas para procesos de fabricación. Actualmente, las tecnologías aplicadas a los procesos de producción son, por un lado, la información digital que está impulsando el uso de la fabricación virtual, y por otro, el mecanizado de alta velocidad orientado a los sectores de la realización de moldes para fundición, a las herramientas de forja y a las herramientas de embutición de chapa. España, en relación con los países de su entorno, dispone de un nivel tecnológico medio en capacidad científica-tecnológica, de producción y comercialización y está por encima de la media en capacidad de innovación.

Técnicas de infraestructura y medio ambiente

La sociedad actual muestra una preocupación creciente por todas aquellas actividades que puedan suponer un deterioro del medio ambiente. Esta preocupación por los temas medio ambientales ha sido asumida por las Fuerzas Armadas que son conscientes de que los materiales que emplean exigen un plan de actuación específico. En este sentido, la línea de actuación que actualmente se está desarrollando se encuentra enmarcada en las áreas sectoriales que se relacionan a continuación:

- Suelos contaminados.

- Planificación y gestión racional de residuos.

- Desmilitarización/destrucción de la munición mediante métodos biológicos.

La protección del suelo es un objetivo ambiental prioritario para las Fuerzas Armadas. En este sentido, la Sección de Defensa Biológica y Toxicología Ambiental del Departamento Nuclear Biológico y Químico (NBQ) de la FNM, en colaboración con grupos de investigación de otros Organismos públicos y privados, está desarrollando proyectos medio ambientales, basados en la detección de sustancias de alto riesgo en suelos, aguas y aire, así como la valoración de riesgo en suelos contaminados y la recuperación de éstos.

En cuanto a la planificación y gestión racional de residuos, el ministerio de Defensa, en colaboración con la industria nacional, y siguiendo una línea de acción en consonancia con la política europea y nacional en esta materia, está buscando nuevas estrategias, de reutilización y tratamiento, que conduzcan a una reducción del volumen y variedad de residuos con el menor impacto medio ambiental y social posible. De esta manera, se ha conseguido una optimización de los procesos de incineración, con límites de emisión muy restrictivos y con un óptimo aprovechamiento energético de los procesos.

Por último, en la desmilitarización/destrucción de la munición mediante métodos biológicos, el Departamento NBQ de la FNM ha desarrollado un proyecto sobre "Biodegradación del TNT por bacterias pseudomonas". En este mismo Departamento, se está trabajando con *microalgas* y *bacterias*, capaces de eliminar

otro tipo de sustancias de alto riesgo, siendo posible su futura utilización como biodescontaminantes.

En relación con el área de infraestructura hay que significar que las Fuerzas Armadas disponen de un importante patrimonio cultural que conviene conservar y mejorar. Por ello es necesario aprovechar los importantes programas de recuperación y restauración que se están llevando a cabo a nivel estatal y autonómico. En estos programas se están aplicando tecnologías avanzadas, para auscultación del estado de los monumentos y rehabilitación de los mismos, que son dominadas por la industria nacional. Por otra parte, las Fuerzas Armadas tienen y utilizan diferentes centros de almacenamiento específicos, distribuidos por la geografía nacional, que se han ido modernizando para cumplir la normativa vigente relacionada con las distancias de seguridad.

Conclusiones

Después de haber expuesto la situación actual en la que se encuentran las tecnologías que se consideran de interés para la defensa, parece conveniente terminar este capítulo sacando algunas conclusiones:

- Hemos visto como evolucionan las tecnologías y la necesidad que se tiene de conocer esos cambios para asegurar que nuestras Fuerzas Armadas utilizan las tecnologías mas adecuadas en cada momento. Para ello es necesario contar con órganos de asesoramiento que lleven a cabo esta misión. Estos órganos son los *observatorios tecnológicos* que están formados por un amplio grupo de expertos, apoyados por un grupo técnico que les da soporte y continuidad, que colaboran, con su conocimiento y experiencia en nuevas tecnologías de aplicación para la defensa, con la DGAM.

- Cada vez es mas frecuente la integración de componentes comerciales en equipos de uso militar (COTS) que permite reducir costes y facilita el mantenimiento. Sin embargo, y en función de la aplicación, es necesario un proceso adaptado de verificación que permita definir los límites de trabajo y fiabilidad de dichos componentes en equipos de uso militar

- El nivel de las tecnologías en las diferentes áreas varía sensiblemente. Nos encontramos con áreas donde el nivel tecnológico de la industria nacional tiene una posición destacada en el concierto internacional y con otras áreas donde el nivel tecnológico es tan bajo que, en caso de ser necesario adquirir estas tecnologías tenemos limitaciones técnicas para hacer una valoración de las mismas. La situación planteada recomienda llevar a cabo dos acciones. En el caso de disponer de una posición destacada, en determinadas tecnologías, con la existencia de tejido industrial y base científica adecuadas, es necesario perseguir el reconocimiento en el concierto internacional que nos consolide en esa posición. Es lo que se denomina adquirir *nichos de excelencia*. Si la situación es de una gran limitación técnica, es necesario conseguir los conocimientos tecnológicos que nos den capacidad básica para saber que los sistemas adquiridos incorporan los niveles tecnológicos adecuados, es lo que se denomina *cliente inteligente*.

- Hemos visto como se ha experimentando un notable incremento en la cooperación, con otros países de nuestro entorno, para llevar a cabo programas internacionales. La situación creada de *cooperación internacional* está fomentando la participación de la industria española y permitiendo el intercambio de información, desde el punto de vista tecnológico, que está siendo muy favorable para el desarrollo industrial. Al mismo tiempo, es necesario arbitrar medidas para racionalizar la *cooperación nacional* que eviten situaciones paradójicas, en las que que, universidades, institutos, y empresas tienen colaboraciones más estrechas con instituciones en el extranjero que nacionales.

Bibliografía

DICCIONARIO DE LA LENGUA ESPAÑOLA. VIGESIMO PRIMERA EDICIÓN. REAL ACADEMIA ESPAÑOLA ,1992.

PLAN NACIONAL DE INVESTIGACIÓN CIENTIFICA, DESARROLLO E INNOVACIÓN TECNOLÓGICA (I+D+I) (2004-2007). http://www.mec.es/ciencia/jsp/plantilla.jsp?area=plan_idi&id=3

PLAN DIRECTOR DE INVESTIGACIÓN Y DESARROLLO (I+D) DEL MINISTERIO DE DEFENSA. http://www.mde.es/dgam/jsp/pdid_i+d.htm

SISTEMA INTEGRADO DE VIGILANCIA AÉREA. http://www.google.es/search?hl=es&q=prototipo+de+uav+del+inta&meta=lr%3Dlang_es

FONDOS DOCUMENTALES DE LA DGAM.

MARTI SEMPERE, Carlos. Tecnología de la defensa. Instituto Universitario “General Gutiérrez Mellado” (UNED) Madrid, 2006

BOLETIN DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA Nº2. PRIMER TRIMESTRE DE 2004.

BOLETIN DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA Nº3. SEGUNDO TRIMESTRE DE 2004.

BOLETIN DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA Nº4. TERCER TRIMESTRE DE 2004.

BOLETIN DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA Nº7. SEGUNDO TRIMESTRE DE 2005.

BOLETIN DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA Nº8. TERCER TRIMESTRE DE 2005.

BOLETIN DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA Nº10. PRIMER TRIMESTRE DE 2006.

CAPÍTULO TERCERO

LA GESTIÓN DE LA INFORMACIÓN COMO ÁREA TECNOLÓGICA DE INTERÉS CRÍTICO: NECESIDADES DE LAS FUERZAS ARMADAS

LA GESTIÓN DE LA INFORMACIÓN COMO ÁREA TECNOLÓGICA DE INTERÉS CRÍTICO: NECESIDADES DE LAS FUERZAS ARMADAS

Por TOMÁS FERRÁNDEZ ARAGÜES

Necesidades emergentes

Las Fuerzas Armadas españolas, así como las Fuerzas Armadas de los países de nuestro entorno, especialmente de la Organización del Tratado del Atlántico Norte (OTAN), NATO en sus siglas en idioma inglés), tienen la necesidad de transformarse para hacer frente a la complejidad, incertidumbres y riesgos que el entorno de seguridad del siglo XXI ha planteado.

Este esfuerzo de transformación se orienta a que las Fuerzas Armadas sean más ágiles, interoperables, proyectables, conjuntas, capaces de ejecutar sus misiones cubriendo un amplio espectro de operaciones diferentes en entornos muy dinámicos.

Estas fuerzas necesitan asimismo adaptarse rápidamente a las circunstancias cada vez más cambiantes e impredecibles, dotándose de unas capacidades que satisfagan y sirvan para cumplir las futuras misiones que se les puedan encomendar. Dichas capacidades deben estar armonizadas con las de las Fuerzas Armadas de los países de la OTAN, así como a las de otros países no pertenecientes a dicha organización y a las de organizaciones civiles.

Para alcanzar todo lo anterior y, lo que es más importante, para que el mando estratégico/operativo pueda decidir en tiempo oportuno y lo más rápidamente posible, nuestras Fuerzas Armadas (y las de otros países), necesitan dotarse de unos medios tecnológicos para gestionar la información:

- Tanto en el nivel estratégico/operativo, para obtener y distribuir eficazmente los datos necesarios que faciliten la toma de decisiones.

- Como en el táctico, en este caso factor crítico para el cumplimiento de la misión.

De manera que la información apropiada pueda llegar desde el más alto escalón de mando hasta el nivel subordinado que se determine en cada momento.

El dominio de la información factor clave

para el éxito de las operaciones

La gestión de la información adquiere una importancia creciente en toda actividad militar. A través de la Historia todos los líderes militares han reconocido que la gestión de la información y, particularmente, la superioridad en la información[24] con respecto a la que posee el enemigo, han sido factores clave para alcanzar la victoria.

Para lograr un adecuado dominio de la información es importante poseer unas comunicaciones seguras y dinámicas, así como lograr la destrucción de elementos de información y comunicaciones enemigos, la protección de elementos propios y de las plataformas que instalen Sistemas de Telecomunicaciones e Información (CIS) o tecnologías de Mando, Control, Comunicaciones y Ordenadores (C4), asociadas a Sistemas ISR o de Inteligencia, Vigilancia y Reconocimiento.

Se hace necesario mantener una clara inferioridad del enemigo en cuanto a obtención de información se refiere, a fin de que tenga el menor control posible sobre lo que en términos anglosajones se denomina SA (*Situation Awareness*) o conciencia de la situación. Para ello no se puede agrandar nuestra esfera de control sobre la base de disponer de más niveles jerárquicos, sino que se debe acortar (aplanar) en lo posible, la cadena jerárquica, lo que redunda en mayor agilidad de la organización y mejoras en los flujos de información, aislando en lo posible este flujo de la cadena de mando para dar más velocidad a la acción en beneficio del ritmo en el planeamiento y conducción de las operaciones.

Llegados a este punto, es interesante recalcar y mantener en la mente el papel de la prensa y los medios audiovisuales en los conflictos modernos: lo mediático hace ganar o perder, hoy por hoy, más de una batalla. Estos aspectos de información

[24] La OTAN definió en 2003 la Superioridad de la Información como la capacidad propia para obtener, procesar y distribuir la información precisa para satisfacer las necesidades de los diferentes escalones de mando, así como para prever los cambios en las necesidades de información del enemigo, al mismo tiempo que se niega al enemigo la capacidad para realizar lo anterior (traducción propia de la definición en inglés).

pública y *mass-media* —Internet— no resultan por tanto cuestiones secundarias en el planeamiento y la conducción de las operaciones.

Se debe asegurar también que, a nivel táctico, se tiene un conocimiento preciso de la situación del campo de batalla, ya que las acciones en este ámbito tienen consecuencias estratégicas (combates en Mogadiscio, bombardeo de la embajada china en Belgrado, lanzamiento de misiles *scud* en la primera guerra del Golfo, etc.).

La situación, planes, potencia de combate, preparación de las fuerzas propias y sus datos logísticos se pueden obtener mediante la transmisión en tiempo oportuno —en ocasiones real— de los datos necesarios empleando Sistemas de Información (SI) y GPS (*Global Positioning System*) apropiados que, además, pueden recibir la información desde los niveles superiores y de otros países. Lo mismo ocurre con los datos meteorológicos, información que puede complementarse mediante los sensores de los sistemas de armas.

Toda esta información sobre la situación debe ser compartida en los diferentes escalones de mando: cuarteles generales, órganos y unidades que tengan necesidad de ella. Asimismo se debe conocer la intención del mando, la doctrina y las capacidades de nuestras fuerzas. Lo mismo ocurriría con las fuerzas enemigas.

Todo lo anterior nos conduce a concluir que debemos formar una red informativa para poder compartir la información requerida.

Importancia de la gestión de la información:

concepto actual de red

Para que toda la información necesaria sea aprovechable, es imperativa la optimización de los procesos de gestión y los flujos de información así como las características de las redes por donde esta información se difunde y comparte.

En la actualidad los ejércitos desarrollan e implantan sus propios Sistemas CIS por medio de los cuales la información es explotada para uso privativo de cada ejército, comprometiendo así la interoperabilidad conjunta y más aún la combinada.

Un ejemplo de ello lo constituye el helicóptero UAV (*Unmaned Aerial Vehicle*) que detecta carros enemigos y transmite la información directamente a una unidad

antiaérea o a un puesto de mando apropiado para ordenar, en tiempo real o casi real, una acción aérea de apoyo aéreo próximo. Queda claro que las acciones en el campo de batalla requieren el entendimiento entre los sistemas, las plataformas de armas, los ejércitos y los aliados. Lamentablemente, la solución al problema no es trivial.

Para compartir información y definir los medios empleados en gestionarla, a finales de los años noventa surgió en Estados Unidos, extendiéndose con posterioridad a otros países, el novedoso concepto de NCW (*Network Centric Warfare*), que en términos OTAN se denomina NNEC (*Nato Network Enable Capability*), o red que consiste, en esencia, en una serie de nodos o entidades enlazados entre sí. En cada nodo se realizan actividades, se recibe la información que, una vez procesada, sirve de base para decidir y actuar y se pone a disposición de otros nodos o entidades el resultado de estos procesos.

Para lograr sus objetivos, la red precisa de una potente red de datos (*data link* o enlace de datos) como herramienta básica para compartir la información entre sensores, plataformas de mando y control y vectores o sistemas de armas.

De esta manera, la información táctica obtenida por un UAV de un país “X” en un teatro de operaciones determinado, podría ser enviada por enlace satélite a su metrópoli para ser retransmitida por fibra óptica submarina a otro país “Y” que a su vez la reenviaría automáticamente por satélite a un tercer país “Z”, quien por enlace LOS (*Line Of Sight*) la haría llegar a un avión AWACS (*Airborne Warning and Control System*) que a su vez y por fin y también por LOS la despacharía hacia sus aviones de combate para el cumplimiento de la misión.

El concepto NNEC (*Nato Network Enuble capability*) permite, entre otros, la dispersión de la fuerza; podemos movernos, recibir apoyo logístico, gestionar mejor los objetivos, reducir riesgos por menores vestigios en el terreno o *footprint* .con el objetivo de conseguir un dominio absoluto de la información con respecto a la del adversario.

Asimismo, y conociendo la intención del mando, nuestras fuerzas tendrán mayor “conocimiento” del espacio de batalla, al estar éste compartimentado.

Habrá también un enlace efectivo entre entidades en el espacio de batalla, por medio de una infoestructura que se materializa en una esfera de información en los diferentes ámbitos político-estratégico, operacional y táctico.

La información del enemigo puede obtenerse de diferentes fuentes: Plataformas de Inteligencia, Reconocimiento y Vigilancia (ISR); como partes de una red de sensores o de sistemas de armas; y HUMINT (inteligencia obtenida por medios humanos).

Para una adecuada explotación de la información, debemos tener unos medios que nos permitan transmitir y actualizar la información entre nodos de la red con una velocidad tal que permita mantener una imagen de la situación -COP (*Common Operacional Picture*)- lo suficientemente puesta al día por los sensores para que, entre otras consecuencias, los diferentes sistemas de armas puedan cumplir con la misión que se les encomiende.

Integración y fusión de información en la red

Como consecuencia de lo anterior, es necesaria la superioridad de la información en operaciones para que actúe como multiplicador de la potencia de combate al conectar en una sola red los sensores, los elementos de mando y control y los sistemas de armas. Ello precisa la integración de dispositivos dispares para obtener, entre otros, un aumento del ritmo en operaciones, una alerta compartida, mayor letalidad y precisión, incremento de la protección, un alto grado de sincronización y un incremento palpable de la velocidad en el ciclo de la decisión.

Asimismo, para evitar errores de los sensores en ambiente operacional, conviene fusionar la información que llegue desde varios de ellos. Un centro de control de sensores debería permitir priorizar las misiones de los sensores, adecuándolas a los cambios de situación, de manera que, fusionando la información recibida, resulte más aprovechable y ello lo sea en el mínimo tiempo. Tal es el caso de la fusión de información procedente de radares en tierra con los embarcados en aeronaves y buques, que permitiría obtener información de blancos móviles terrestres de los que no se pudiera realizar su seguimiento desde tierra por problemas meteorológicos o de falta de enlace directo debido a los accidentes del terreno.

Lógicamente la información que reciben los diferentes sensores debe ser transmitida a una gran velocidad por una infraestructura de información capaz de priorizar el transporte y el proceso de la información, es decir, con una gran QoS (*Quality of Service*) o calidad de servicio.

Se trataría también de que los centros de mando y control de las unidades dispongan de un mejor conocimiento de la situación, de que los sensores respondan mejor a las necesidades de información requeridas y de que se disminuya la firma radar y la huella electromagnética de los diferentes centros y órganos de mando y de ejecución.

Por otra parte, manteniendo en red a los sensores y sistemas de armas podemos evitar el fuego fratricida, tan negativo para el combate moderno, pues no sólo se causan bajas propias, sino que se afecta a la moral de las fuerzas y a la imagen mediática del despliegue.

Además, la infraestructura de la red debe acercar virtualmente los centros de planeamiento y de simulación, de manera que se puedan diseñar las operaciones con los parámetros y condiciones previstas, a la vez que se ensayan y simulan las condiciones de la operación, posibilitando los estudios de sensibilidad ante las distintas hipótesis de trabajo y la información actualizada permanentemente.

Del dominio de la información al dominio del conocimiento

Este dominio de la información implicará también un «dominio en el conocimiento», es decir, una ventaja con respecto al enemigo en los procesos de preparación de la fuerza antes de su empleo. Esa ventaja en el conocimiento anticipado afectará a todas y cada una de las actividades y funciones de la preparación.

El mando de doctrina del Ejército de Tierra señala, al hablar del campo de batalla futuro ([25]), que la gestión del conocimiento trata de alcanzar, frente al enemigo, la superioridad en el uso y manejo de la información, o mejor, gestionar la inteligencia

[25] MADOC: Campo de Batalla Futuro 2005. Varios párrafos anteriores están tomados de este documento.

con superioridad. La integración de los sistemas basados en procesos digitales o entidades de conocimiento, en un sistema gestor, proporcionará en el espacio de batalla:

- Una mayor precisión en el conocimiento de la situación y de los efectos producidos, antes, durante y después de las acciones.
- Gran velocidad en la observación de la realidad y en la toma de una decisión.
- Mayor agilidad, eficiencia y rapidez en la agrupación y/o dispersión de los recursos empleados.

La gestión del conocimiento obliga también a compartir la información de la situación entre las diferentes unidades del espacio de batalla. Pero compartir no significa necesariamente la misma difusión en todos los escalones. Una tarea obligada de esa gestión del conocimiento será compartimentar, estructurar y catalogar la información, proporcionando a cada escalón aquello que verdaderamente interese.

En este sentido, la esfera de la información táctica a que nos referíamos anteriormente tiende, en función del estado del arte de los medios disponibles, a la obtención de información bajo demanda o información que se obtiene a través de la *web* y que actualiza la situación de las fuerzas propias por medio de GPS o sistema de situación global que, embebido en un sistema de información FFT (*Friendly Force Tracking*), envía la información hacia el Sistema de C2. Las unidades, vehículos de combate y combatientes seleccionados (dotados de los medios del combatiente futuro) deben tomar parte de esta actualización de la base de datos de la *web*.

Esta información debe ser compartida por los medios C-2 que lo necesiten e introducida en la Infosfera o esfera de la información que, como se ha dicho, abarca los diferentes ámbitos estratégico, operacional y táctico.

La situación enemiga se conoce por medio de los diferentes sensores que deben integrarse en el Sistema C2. Así pues se genera automáticamente la situación SA (*Situation Awareness*) que es filtrada y consolidada de una manera jerárquica.

Cada jefe de escalón de mando así como cada oficial de los cuarteles generales debe tener acceso en todo momento a la información que necesita para cumplir su

misión. Dicha información debe ser compartida de tal manera que le llegue de forma transparente al usuario, sin que exista impedimento alguno por barreras organizativas o de sistemas ni por las exigentes medidas de seguridad de la información, necesarias especialmente en la interconexión de los Sistemas CIS con países aliados o componentes de una coalición.

Cabe hacer mención aquí a una de las dificultades a las que se enfrenta en concepto de red táctica: la eliminación de la información basura, la mensajería no prioritaria y la presencia en el medio de otros “ladrones de recursos”, que deben ser convenientemente gestionados, lo que lleva de inmediato al problema más grave del concepto NNEC: la seguridad de la red y los recursos que ésta requiere.

Durante años, las fuerzas terrestres han ido a la zaga de las aéreas y navales en la implantación de las tecnologías C4. El complejo entorno operacional, los problemas de la diversidad de plataformas, las limitaciones de movilidad y la falta de la adecuada capacidad de transferencia de datos, principalmente en el ámbito táctico y debido a comunicaciones en banda estrecha, mantuvieron a las fuerzas terrestres lejos de usar los Sistemas C4 integrados, mientras que no se obtenía el rendimiento adecuado de los sistemas utilizados en los ámbitos estratégico y operacional, debido fundamentalmente a la falta de flujo de información procedente de los escalones subordinados. De esta manera se dificultaba la interoperabilidad conjunta y más aún la combinada.

Por ello y dado que en la actualidad los ejércitos desarrollan e implantan sus propios Sistemas CIS, necesitamos aprovechar los medios que tenemos, hacerlos evolucionar e integrarlos para que formen una red tupida de gestión de información en los que estén integrados, por medio de una infraestructura y de unos procedimientos, los puestos de mando, las unidades, los sensores o medios de obtención de información y las plataformas y vectores de tiro.

La necesidad de despliegue de medios, fundamentalmente los medios de entrada inicial y más adelantados en el despliegue del componente terrestre, y la falta de las suficientes capacidades en ancho de banda, implican ciertos problemas en el volumen de información que puede ser compartida por los diferentes escalones de mando.

Ello demandará inversiones en medios CIS para poder abandonar y evolucionar progresivamente y sin solución de continuidad los actuales Sistemas CIS de mando y control utilizados por los Ejércitos y la Armada, así como por el Estado Mayor de la Defensa, para obtener otros que, basados en la arquitectura técnica de mando y control definida por el Plan Director CIS permitan que desde todos los niveles de mando se pueda acceder a la información necesaria para el mejor cumplimiento de la misión ([26]).

Posteriormente nos referiremos particularmente a los Sistemas CIS y a las tecnologías C4 aplicadas al entorno aeroterrestre táctico, por integrar todas las que nos interesan en este estudio. En la actualidad los ejércitos desarrollan e implantan sus propios Sistemas CIS por medio de los que la información es utilizada primordialmente para uso de cada Ejército, dificultando la interoperabilidad conjunta y, más aún, la combinada.

Factor esencial: la seguridad de la información

Particular atención debemos prestar en los aspectos de la Seguridad de la Información (INFOSEC) ([27]). Los procedimientos, aplicaciones y sistemas de cifrado de INFOSEC deben asegurar que la información precisa llega a la persona adecuada en el momento oportuno, así como que se garantiza la integridad de dicha información. Por ello debemos encontrar un equilibrio entre “necesidad de conocer” y “deber de compartir”. Esta última premisa asegura que las políticas, los procedimientos y los sistemas están desarrollados y serán implantados con unas capacidades intrínsecas de compartir información, pero también con los mecanismos de seguridad necesarios para gestionar dinámicamente los permisos de acceso y asegurar que tan sólo los usuarios autorizados pueden acceder a la información.

---

[26] Históricamente, los niveles estratégico, operacional y táctico existen por las limitaciones en las comunicaciones y en las esferas de control. Si rebajamos estas limitaciones, se podría plantear el cambiar el reparto de responsabilidades de los niveles de conducción de la guerra u operaciones.

[27] En la actualidad se emplea el término, más amplio que el de INFOSEC, *Information Assurance* o confianza, garantía y seguridad de la información, dentro del concepto de operaciones en red, que garantiza la disponibilidad, integridad, confidencialidad, autenticación, identificación y no repudio en la gestión de la información, prohibiendo el acceso a la misma de las fuerzas hostiles.

Necesidad de un área tecnológica

Para la gestión de la información

Los medios tecnológicos mencionados deben asegurar la interoperabilidad entre las fuerzas propias y las aliadas, proporcionar fluidez y rapidez a los procesos de mando y control, capacitar a las Fuerzas Armadas para adaptarse a los cambios en la situación operativa permitiéndoles cumplir varias misiones simultáneas sobre diferentes escenarios sin perder por ello flexibilidad, y cumplir unos requisitos de normalización que les permitan incorporar las nuevas capacidades que la industria vaya logrando.

Estos medios tecnológicos los podríamos englobar en un área tecnológica que permitiera a nuestras Fuerzas Armadas:

1. Mejorar el proceso de la decisión ([28]), llegando al dominio y superioridad de la información y de la gestión del conocimiento del campo de batalla (*Decision Superiorita*) ([29]).

   - Mediante el acceso a un amplio abanico de fuentes.

   - Proporcionando al mando en tiempo oportuno la información necesaria al más alto nivel.

   - Mejorando el ritmo en la toma de decisiones, lo que exige una inteligencia capaz de aportar los datos que las fundamenten a una velocidad y con una precisión cada vez más elevadas. La integración de los jefes de las unidades de cada nivel con el comandante del nivel superior debe ser la base que permita componer un conocimiento constante y preciso de la situación tanto operativa como logística para huir de procesos de planeamiento largos y complejos, que proporcionarían la ventaja “decisional” al enemigo.

[28] NATO NNEC Vision and Concept. 06-02.06

[29] “The application of knowledge by commanders to make quality decisions directing assigned forces and harnessing additional support at the right time such that they preserve operational flexibility and maintain the initiative in the battlespace”. (NATO NNEC *Vision and Concept*)

- Enlazando sensores, los C2 de los cuarteles generales y unidades, las plataformas y los apoyos (sistemas de armas) para lograr una sinergia en la capacidad operativa.

- Optimizando el apoyo a la decisión y el proceso de planeamiento.

- Mejorando y acrecentando los enlaces para el intercambio de información con las organizaciones civiles, tanto nacionales como internacionales –Organizaciones No Gubernamentales y Organizaciones Internacionales-.

- Intercambiando información entre las diferentes "comunidades de Interés" o áreas funcionales (operaciones, logística, inteligencia, cooperación civil-militar, etc.

2. Mejorar las capacidades de nuestras Fuerzas Armadas.

Proporcionando enlaces que permitan aumentar la coordinación operativa ejemplo: COP y la sincronización de las acciones. También proporcionando, entre otros y sin relacionarlos por orden de importancia:

1. Un rápido flujo de información para mando y control entre las áreas funcionales de los cuarteles generales fijos y desplegables que, además de mejorar el empleo directo de las fuerzas propias, dé la suficiente flexibilidad que permita adaptarse a la situación.

2. Sistemas de comunicaciones que permitan intercambiar información entre nuestras Fuerzas Armadas y las de nuestros aliados.

3. Un alto grado de interoperabilidad en las redes de comunicaciones –o infraestructura de redes e información NII en su denominación OTAN- para alcanzar las capacidades operativas que se fijan a las Fuerzas Armadas. De esta nueva filosofía emanan conceptos como la federación de sistemas, la arquitectura orientada a servicios, cifrado de todas las redes (*Black Core Network* o *All Encrypted Network*), mínimo número de *interfaces*, etc. Por ejemplo, el concepto de *Black Core Network* se define como la infraestructura en la cual todo el tráfico se transporta cifrado de manera que sea más sencillo interconectar sistemas de diferentes dominios. En principio, todas las redes deben migrar hacia él, lo que

supone que la gestión de redes y cifradores se debe poder realizar, así como que debe existir interoperabilidad de los cifradores, debe estar superada la problemática de acreditación de sistemas y la gestión de claves, etc, lo que no es posible a día de hoy por no disponer de la suficiente madurez tecnológica en este aspecto.

4. El favorecer el trabajo de los órganos de Inteligencia al poder crear productos procedentes de la fusión de información de varias fuentes, así como su rápida y fácil distribución.

5. Los procedimientos de obtención, que se apoyarán, tanto en una red digitalizada que funcionará con sensores en las tres dimensiones y en ámbitos electromagnético, cibernético, nuclear, biológico y químico y antiterrorista —en cuanto a detección de dispositivos explosivos y protección física de los nodos de la red—, como en el trabajo de equipos humanos, imprescindibles en determinadas tareas de inteligencia y en ambientes que, como el urbano y el que se produce en áreas poco desarrolladas, tienen en el establecimiento de redes personales la clave del éxito. La actuación de los Vehículos Aéreos no Tripulados (UAV) y una completa red de sensores será determinante.

6. El favorecer la ejecución de una operación a nivel operacional-táctico mediante el apoyo previo en difusión del conocimiento de los órganos de planeamiento estratégico-operativo.

7. Sistemas CIS que permitan operaciones fuera del teatro nacional y que puedan integrarse y ser interoperables con sistemas de países aliados.

8. El favorecer la maniobra conjunta y combinada, incluso con elementos con poca capacidad de información, al utilizar la conectividad necesaria, lo que conlleva a aumentar la protección de la fuerza y reducir los tiros fratricidas.

9. La capacidad de optimizar el proceso de *Targeting*, transmitiendo rápidamente la información de objetivos directamente desde los elementos de primera línea a los órganos decisorios para el empleo del apoyo de fuego conjunto más apropiado y para conseguir un efecto determinado.

10. La posibilidad de reducción de órganos logísticos en la zona de operaciones, al conocer en tiempo casi real la situación actualizada y el estado de los abastecimientos necesarios para la operación.

11. La capacidad de apoyo sanitario y vigilancia de enfermedades y tratamientos.

12. Consultas interactivas entre autoridades, a nivel estratégico y combinado, para favorecer la vigilancia y gestión de crisis.

Requisitos del área tecnológica de gestión de información

Los medios necesarios para establecer la infraestructura de este área tecnológica de los medios CIS y de los Subsistemas CIS asociados a los medios Reconocimiento, Inteligencia y Vigilancia (ISR) deben satisfacer, entre otros, los siguientes requisitos:

- Sencillez para los operadores. Empleo de *interfaces* con o sin teclado con funciones predeterminadas y mensajes breves como resultado de procesos complejos.

- Rapidez en la transmisión de la información: Las acciones se desarrollan cada vez con mayor rapidez y se deben tomar decisiones casi en tiempo real por personas muy alejadas unas de otras. En este sentido, unas veces el tiempo real requerirá la inmediatez en la transmisión, mientras que en otros se admitirán periodos de latencia superiores a varios minutos.

- Integración con otros sistemas: los sistemas no pueden trabajar aisladamente, sino que deben integrar información de otros.

- Interoperabilidad: los equipos deben operar con otros, sean propios o de los aliados en diferentes configuraciones.

- Seguridad: los sistemas deben ser concebidos desde su inicio de manera que sean intrínsecamente seguros, con técnicas de autenticación, corrección de errores y cifrado.

- Redundancia de la información y redes: se debe reducir la probabilidad de fallos manejando datos con orígenes diferentes que se transmitan por redes de comunicaciones diferentes.

- Estructura de red muy descentralizada, manteniendo la decisión centralizada.

- Funciones automatizadas: limitar la necesidad de operadores a tareas de mantenimiento, supervisión y decisión, haciendo que muchas operaciones sean transparentes para el usuario.

- Preparación técnica de operadores: paradójicamente, la capacitación de estos últimos tendrá un perfil más técnico que en la actualidad, a pesar de la sencillez que supondrá para ellos el manejo de los sistemas, debido a las mayores capacidades de los mismos, lo que exigirá una preparación técnica también superior a la actual. En todas las ocasiones existirá la presencia humana en la decisión (*man in the loop*) y pocas serán las órdenes de fuego o que impliquen violencia generadas de manera automática.

Para satisfacer las características anteriores, se duplicarán en el futuro casi todas las redes por las que discurren tanto la información de los sensores como las órdenes de mando y control para asegurar su inmunidad a fallos. Del mismo modo, el *hardware* de los centros de mando y control tendrá que ser de elevadas prestaciones en términos de rapidez de proceso, fiabilidad y disponibilidad a partir del uso masivo del proceso paralelo y la vectorización de la información. Por su parte, el *software* deberá ser multitarea, capaz de realizar procesos en tiempo real o casi tiempo real e implementará técnicas avanzadas de fusión de datos e inteligencia artificial ([30]). Los centros de mando y control se estructurarán de manera distribuida pero perfectamente coordinados entre sí, con una delimitación clara de jerarquía y responsabilidades.

En lo que afecta a la guerra electrónica, la eficacia de los sistemas dependerá en gran medida del conocimiento del modo de trabajo de sus distintas amenazas y de los sistemas de cuya acción puedan ser objeto, para dotar a los sistemas propios de adaptabilidad, inteligencia y comunicaciones (por las que recibirán datos obtenidos por otros sistemas, como por ejemplo los sensores y sistemas de inteligencia y guerra electrónica).

---

[30] Las matrices de fusión representan una complejidad técnica formidable, sobre todo cuando las información que se procesa es de tipo gráfico.

Los requisitos de los nuevos sistemas asociados a las aplicaciones de seguridad y defensa son imposibles de obtener sin la conjunción de las tres tecnologías básicas que intervienen en ellos: electrónica, informática (*software*) y comunicaciones.

Entorno de aplicación del área tecnológica

de gestión de información

La infraestructura que posibilita el intercambio de información se debe implantar desde los centros de decisión del escalón de mando más elevado o de alto nivel Presidencia del Gobierno, Junta de Defensa Nacional, Ministerio de Defensa, mando de operaciones, etc., hasta el ámbito táctico de las unidades en operaciones.

Gestión de la información de alto nivel: plataforma tecnológica corporativa

En la actualidad, los Sistemas de Telecomunicaciones del Ministerio de Defensa se conciben como una Red Global de Telecomunicaciones (RGT), definida como una única red formada por dos dominios:

1. Recursos externos al Ministerio de Defensa (telecomunicaciones de propósito general). Este dominio incluye los medios de telecomunicaciones que ofrecen servicios de voz y datos a todos los usuarios del Ministerio de Defensa y son contratados a operadores públicos. Estos servicios son gestionados por el Centro Corporativo de Explotación y Apoyo (CCEA) y se basan en Redes Privadas Virtuales (RPV) para voz, fija y móvil, y para datos.

2. Recursos propios del Ministerio de Defensa (telecomunicaciones de mando y control). Este dominio está formado por los recursos propiedad del Ministerio de Defensa que dan servicios de telecomunicaciones a los usuarios de mando y control. Los recursos propios fundamentales que ofrecen servicios de telecomunicación son:

   – Red Conjunta de Telecomunicaciones (RCT) del Sistema Conjunto de Telecomunicaciones Militares (SCTM). Red militar a nivel nacional que llega a los principales emplazamientos del Ministerio de Defensa y que, a través del Sistema Español de Comunicaciones Militares por Satélite (SECOMSAT), ofrece enlaces vía satélite. Es una red multiservicio de alta disponibilidad para paz, crisis o conflicto armado, y cuya obtención, administración, operación y

mantenimiento es responsabilidad de las Fuerzas Armadas. La gestión de la RCT del SCTM la realiza el Centro de Gestión del Sistema (CGS), dependiente del Estado Mayor de la Defensa.

- Redes de Telecomunicaciones Tácticas de las Fuerzas Armadas. Son gestionadas y explotadas por los Ejércitos y la Armada.

En lo relativo a Internet, se dispone de un punto único de acceso a Internet con alta disponibilidad y gran seguridad física y lógica, que proporciona los servicios de navegación corporativa, correo electrónico externo y hospedaje de páginas *web*.

La configuración de las redes de área extensa será de dos redes WAN físicamente aisladas:

- WAN para mando y control militar, que se interconectará con entornos tácticos.

- WAN corporativa de propósito general, que se extenderá a las estaciones de trabajo del Ministerio de Defensa, cuya explotación se gestionará, como se ha mencionado, de forma centralizada en un único CCEA.

La WAN corporativa de propósito general dispondrá de un repositorio único de información, accesible tanto por aplicaciones como por usuarios, que constituirá el directorio corporativo, que será esencial para el funcionamiento de la infraestructura de seguridad basada en la Infraestructura de Clave Pública (PKI) y la tarjeta electrónica militar desarrollada como un proyecto Investigación, Desarrollo e innovación (I+D+i) en colaboración con el Centro Nacional de Inteligencia.

En lo relativo a seguridad, la dirección y gestión de seguridad se llevarán a cabo mediante unas directrices comunes, materializadas por la Política de Seguridad de la Información aprobada por el Ministerio y la implantación de las ya mencionadas tarjeta electrónica militar y la implantación de una PKI.

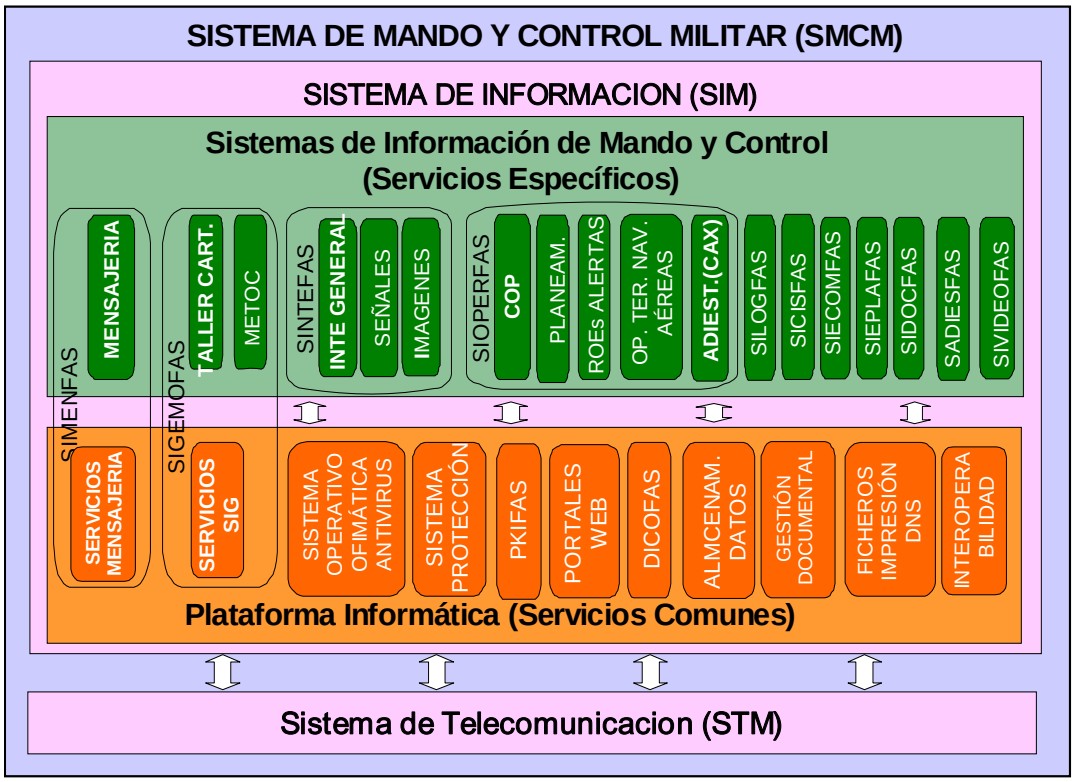
En cuanto a los Sistemas de Información en el ámbito del Ministerio de Defensa, la situación actual viene impuesta por el Plan de Obtención y Modernización de los Sistemas de Información de Defensa. En lo que al área de mando y control se refiere, se está realizando la definición del Sistema de Mando y Control Militar (SMCM) plasmada en conceptos y arquitecturas de referencia de los sistemas que lo

componen, como guía a todo el ciclo de vida de los mismos. En el cuadro insertado más abajo se puede observar la composición del SMCM.

Los principales proyectos de sistemas de información dentro de esta área de mando y control, a los que dará soporte su respectiva plataforma de telecomunicaciones son los siguientes:

- Sistema de Mensajería Militar (SIMENFAS).
- Sistema de Videoconferencia Militar (SIVIDEOFAS).
- Sistema de Inteligencia de las Fuerzas Armadas (SINTEFAS).
- Subsistema de Inteligencia General.
- Subsistema de Captación de Señales Electromagnéticas y Ópticas.
- Subsistema de Gestión y Tratamiento de Imágenes.
- Sistema de Apoyo a la Conducción de Operaciones (SIOPERFAS).
- Subsistema de Planeamiento Operativo.
- Subsistema de Gestión de Alertas y Reglas del Enfrentamiento.
- Subsistema para la Generación y Gestión de la COP.
- Subsistema de Conducción de Operaciones Terrestres (SIAOT).
- Subsistema de Conducción de Operaciones Navales.
- Subsistema de Conducción de Operaciones Aéreas.
- Subsistema de Ejercicios Asistido por Ordenador.
- Sistema de Gestión y Coordinación Logística de Operaciones (SILOGFAS).
- Sistema de Gestión del Apoyo CIS a las Operaciones (SICISFAS).
- Sistema de Gestión Cartográfica, Meteorológica y Oceanográfica (SICAMOFAS).

- Subsistema para la Gestión y Distribución de la Información Cartográfica.
- Subsistema para la Gestión y Distribución de Información Meteorológica y Oceanográfica.
- Sistema de Estrategia y Cooperación Militar (SIECOMFAS)
- Sistema de Planeamiento de la Fuerza (SIPLAFAS).
- Sistema de Gestión y Difusión de la Doctrina (SIDOCFAS).
- Sistema de Planeamiento, Gestión y Evaluación del Adiestramiento y Preparación de la Fuerza (SADIESFAS).
- Subsistema de Adiestramiento Conjunto.
- Subsistema de Adiestramiento y Preparación de la Fuerza Terrestre.
- Subsistema de Adiestramiento y Preparación de la Fuerza Naval.
- Subsistema de Adiestramiento y Preparación de la Fuerza Aérea.



Para mando y control, esto es, con fines operativos, las Fuerzas Armadas deberán emplear una Arquitectura Orientada a Servicios (SOA) que se implemente principalmente por servicios *web*, o *webservices* (WS), que son servicios ofrecidos por una aplicación a otras aplicaciones. Estos servicios *web* utilizan estándares básicos, como XML (*eXtensible Markup Language*) para el intercambio de datos, lo que facilita la utilización de cualquier plataforma SW/HW (*Software/Hardware*), ya que este lenguaje de marcas o *tags* que usa el estándar ISO 8879 simplificado, facilita y hace que la información sea transportable entre sistemas distintos. Asimismo, la comunicación entre el cliente o usuario y el servicio se podrá hacer utilizando el protocolo SOAP (*Simple Object Access Protocol*), así como el WSDL (*Web Services Description Language*) o lenguaje de descripción de servicios disponibles y el UDDI (*Universal Description, Discovery & Integration*), para identificación, publicación y localización de servicios disponibles, figura 1.

De esta manera, dispondremos de una información actualizada que podremos compartir y que podrán usar continuamente las células de planeamiento y otros elementos que tengan esa necesidad de conocer. El puesto de mando podrá ser virtual y el Jefe estar separado físicamente de su estado mayor o *staff*, de manera que los componentes del mismo estén en la posición desde la que puedan efectuar, en las mejores condiciones, su trabajo individual.

Los principales proyectos de sistemas de información corporativos a los que dará soporte la plataforma de telecomunicaciones de propósito general son los siguientes:

1. Mensajería oficial y gestión documental (oficina virtual sin papeles).

2. Sistema de Gestión del Conocimiento, que consistirá en:

   - Intranet basada en servicios en lugar de basada en la navegación.

   - Establecimiento de “campus virtual” que permita el aprendizaje permanente.

   - Comunidades de prácticas y grupos de trabajo virtuales para favorecer la colaboración en una organización dispersa geográficamente.

3. Sistema de Gestión Económica.

4. Sistema de Gestión Sanitaria.

5. Sistema de Gestión de Infraestructura.

6. Sistema de Gestión de Recursos Humanos.

Gestión de la información en redes operacionales/tácticas. Necesidades

Las redes de telecomunicaciones tácticas tienen tres factores que añaden complejidad frente a las redes corporativas y civiles:

- Requisitos operativos particulares de las Fuerzas Armadas, como seguridad, movilidad e interoperabilidad.

- Características técnicas y servicios particularizados a las necesidades de las Fuerzas Armadas, como por ejemplo la necesidad de recursos en comunicaciones por RDSI (*Red Digital de Servicios Integrados*).

- Limitaciones del Ancho de Banda.

La conectividad necesaria para la gestión del flujo de información con los escalones superiores es elevada, por lo que se deben utilizar comunicaciones basadas en tecnología IP (*Internet Protocol*) sobre radio enlaces de banda ancha, incluyendo tecnologías ATM o redes WIMAX, que proporcionen velocidades de 54 Mbps en una zona de 50 kilómetros. Esta conectividad y ancho de banda debe ser mantenido para integrarse en los escalones superiores por medio de radio enlaces o enlaces satélite. La conectividad necesaria hacia escalones subordinados la proporcionarán radio enlaces y radios con capacidades de hasta 512 Mbps o incluso por medio de enlaces satélite.

Siempre que los medios y la seguridad lo permitan, se debe emplear conectividades basadas en el protocolo IP, ya que permite una mejor y más económica integración de la información procedente de diferentes fuentes con los medios disponibles.

Las comunicaciones militares han aprovechado el rápido desarrollo de las comunicaciones comerciales, de la telefonía móvil y de la tecnología IP. Esto hace que parte de la infraestructura de las comunicaciones militares debe estar basada en productos COTS, que incluyen teléfonos móviles de tercera generación y Sistemas

Tetra y Tetrapol y Voz sobre IP (VoIP v.6). La tecnología está permitiendo remplazar los tendidos alámbricos entre y dentro de PC por inalámbricos que utilizan protocolos Wimax y Wifi (IEEE 802.11E). Estas últimas tecnologías permiten desplegar los puestos de mando en una zona amplia de manera que no puedan ser detectados fácilmente desde el aire por el voluminoso despliegue de sus medios o por su firma electrónica.

A nivel brigada, se requiere una mayor capacidad de gestión de información y de inteligencia en tiempo real, a la vez que se necesita acceso a los medios de inteligencia de los escalones superiores ([31]).

Las redes de mando y control transmiten informes periódicos por medio de mensajes preformateados, de manera que los escalones subordinados pueden informar a los superiores sobre su situación táctica automáticamente. Estos informes deben incluir la situación geográfica de las unidades así como el estado y la disponibilidad de los abastecimientos, niveles de munición en cada vehículo de combate, estado del sistema sanitario, etc. Los informes reflejan el momento en el que se redactan y la posición del redactor, para facilitar y colaborar en la formación de la RLP

---

[31] Como ejemplo, en el Ejército de los Estados Unidos, la Brigada "*Stryker Brigade Combat Team*" utiliza las capacidades que ofrece el concepto antes definido de Network Centric Warfare NCW por medio, fundamentalmente, de sus cinco redes CIS.

- Para enlazar con los escalones de mando superiores, la red de enlace TSC-154 SMART-T por satélite MILSTAR con una velocidad de 1,5 Mbps., utilizada para planeamiento, transmisión de órdenes, productos de inteligencia y superponibles de situación.

- Red de radio enlaces (Near Term Digital Radio System NTDRS) de 28,8 kbps que enlaza los puestos de mando de la Brigada y de sus unidades subordinadas, también y como la anterior, para transmisión de órdenes

- Red de Internet Táctica (*Enhanced Position Location Radio System EPLRS*) de 14,4 a 56,6 kbps, que transporta la información sobre la situación de las unidades y la mensajería de la Brigada, también por radio enlaces.

- Red Radio de Combate (CNR, o de voz en FM (modulación en frecuencia), utilizada en todos los escalones de mando de la Brigada

- GBS o *Global Broadcast System*, red de enlace satélite (de hasta 24 Mbps por transpondedor), para transmisión de vídeo, imágenes desde las agencias de información nacionales

También se cuenta con una red de enlace satélite TACSAT PSC-5 Spitfire de 16kbs de enlace de PC,s, así como otra de radio enlaces (BSN-HCLOS) a 8192 Kbs para transmisión de datos entre el PC de la Brigada y su unidad de apoyo logístico y medios específicos de comunicaciones para enlace con los órganos de inteligencia nacionales y para transmisión de imágenes desde los UAV,s.

(*Recognised Land Picture*) de nivel brigada y superiores, que a su vez contribuirá a la edición de la COP.

Para la generación de situación logística, se puede realizar manualmente o de forma automática utilizando la tecnología RFID.

Los medios C4 integrados en vehículos blindados de combate, artillería autopropulsada y helicópteros, deberán incluir los sistemas de control de fuegos, equipos electro ópticos, sistemas de navegación, radio e intercomunicadores, contramedidas, de manera que se conecten los sistemas de armas con los de información por medio de enlaces de datos (*data link*)

Los modernos vehículos de combate están equipados con medios CIS que posibilitan el intercambio de información entre los miembros de la tripulación, especialmente entre el jefe, conductor y tirador, creando una red LAN por medios de un *switch*, *router,* servidor y clientes (pantallas táctiles). A medida que aumenta el escalón de mando, los sistemas muestran una información más completa y discriminada por medio de los filtros correspondientes.

También deben estar equipados con modernas pantallas o *displays* para hacer más segura la conducción del vehículo, sobre todo por la noche.

En el escalón inferior, la red radio de combate portátil y vehicular junto con los medios CIS del combatiente de futuro, permitirán, por medio de la red de comunicaciones apropiada -actual Red Básica de Área (RBA)-, conectar a los combatientes y sus medios vehiculares con los escalones de mando superiores.

La seguridad de la información INFOSEC, como se ha mencionado anteriormente) adquiere particular importancia, tanto para la información en sí misma como para los medios CIS. Se deben tomar las medidas de protección adecuadas para impedir la intrusión, denegación de servicio, explotación y cualquier tipo de ataques llevados a cabo por virus, troyanos o gusanos informáticos.

También se emplearán, aunque aún están en desarrollo, redes de área móviles MANET (*Mobile Area Networks*) que podrán autoconfigurarse para adaptarse a las necesidades del despliegue.

Características técnicas de las redes tácticas

Las redes militares tácticas deberán ser intrínsecamente seguras, muy flexibles, de operación sencilla, fácil y rápidamente desplegables, con elevada capacidad de supervivencia y recuperación del servicio, merced a su tolerancia ante fallos y ante destrucciones parciales, capaces de soportar transmisión de voz y datos para aplicaciones en tiempo real, con protocolos y arquitecturas robustos, con corrección de errores y medidas de protección como el salto en frecuencia, que trabajen en entornos distribuidos, fáciles de mantener.

Los sistemas de Información para mando y control empotrados en Sistemas de Armas exigirán el intercambio de información, principalmente en forma de bits de datos, vía radio en tiempo real o casi real, lo que llevará cada vez más al aumento de las frecuencias empleadas, con el fin de ampliar el ancho de banda disponible (a costa de aumentar la potencia transmitida o una reducción en el alcance del enlace radio), así como al empleo de protocolos de acceso al medio eficientes que garanticen un tiempo máximo de acceso acotado en un intervalo aceptable, como por ejemplo protocolo de paso de testigo con multiplexación por división en el tiempo, como *Token Ring* y TDMA, respectivamente.

Los Sistemas de Información para el Mando y Control no embebidos en Sistemas de Armas, al igual que éstos, deben ser interoperables, en especial con las redes de mando y control de los países aliados y amigos. Para ello, el objetivo ideal es que una unidad dotada de los sistemas propios se integre en una fuerza internacional como *Plug and Play* con acceso en tiempo real y que no requiera procesos manuales o transformadores de datos de tipo alguno, por ejemplo mediante el empleo de un modelo de datos común o el acceso a los servicios de datos normalizados, mediante suscripción.

Los sistemas de radio tácticos, en un futuro inmediato, tenderán al empleo de redes homogéneas de tipo Intranet en IP v.6 con arquitectura *web* y podrán beneficiarse del concepto de redes asimétricas que ya se han puesto en marcha en otros ámbitos del mundo civil. Este tipo de redes, conocidas como GBS (*Global Broadcasting System*) se basa en el concepto de que el usuario normalmente recibe mucha más información de la que envía. Por ello, se puede mejorar el aprovechamiento del

ancho de banda mediante el empleo de un canal de subida desde el terminal del escalón inferior sobre un circuito estándar de bajo ancho de banda y de un canal unidireccional de bajada sobre señal digital de difusión directa satélite. El resultado es equivalente al de una red IP asimétrica que a los efectos del usuario final es una red de elevado ancho de banda.

Las propuestas iniciales de uso de arquitectura *web* en el ámbito militar táctico europeo se han visto empañadas por la opinión extendida de falta de seguridad en la arquitectura *web* y la confusión de que tecnología *web* y conexión física a Internet son lo mismo. No obstante, la tecnología PKI y la incorporación de extensiones de cifrado JCE en JAVA con la aplicación de firmas digitales tanto para datos como para código, las listas de control de accesos y la definición de dominios protegidos, conforman una panoplia de herramientas con capacidades suficientes para alcanzar el nivel de seguridad requerido en aplicaciones militares.

Los sistemas basados en servicios *web* exigen enlaces con un ancho de banda y disponibilidad considerables. En la práctica, esto se puede resolver en gran medida mediante la utilización de sistemas WAP con acceso inalámbrico y velocidades inferiores a 9600 bps para el intercambio de datos alfanuméricos e imágenes de baja resolución y el uso de redes asimétricas. De acuerdo con ello, los servicios WAP (*Wireles Application Protocol*) sobre *web* WML (*Wireless Markup Language*) y puertas de enlace WAP para acceso de móviles y PDA (*Personal Digital Assistant*) extienden el uso de la arquitectura de red a los dispositivos móviles de mano con una posible aplicación en las redes tácticas de combate y redes HF (alta frecuencia) de bajo ancho de banda.

Una serie de condicionantes llevan a un aumento del empleo de las comunicaciones por satélite, tanto con satélites militares como comerciales, y su acercamiento hasta escalones tácticos inferiores, como batallón y compañía, incluso para el caso de terminales satélite móviles. Entre ellas encontraríamos las dificultades de establecimiento de enlaces HF en función de las condiciones ambientales y de distancia (tanto en operaciones en áreas lejanas como en el segmento de distancia de 60 a 120 kilómetrso aproximadamente), la vulnerabilidad de la banda de frecuencias HF por ser frecuencias bajas y por tanto muy accesibles para el nivel alcanzado por la electrónica actual empleada en equipos de guerra electrónica

(incluso con medidas de protección electrónica o EPM), la dificultad para el establecimiento de comunicaciones HF en movimiento por el efecto *doppler* y la necesidad de planos de tierra eficientes en las antenas, el escaso ancho de banda para datos disponible en la banda HF y la mayor seguridad de las comunicaciones por satélite,

Los sistemas e infraestructuras críticas de telecomunicaciones no pueden confiarse a una única solución tecnológica. Deberá asegurarse la disponibilidad de alternativas con estructuras redundantes claramente diferenciadas que permitan transferir la operación de infraestructuras críticas de una a otra de forma rápida y sencilla. En este momento la tecnología de posicionamiento y sincronización depende de una única fuente de información: el GPS, extremadamente sensible a contramedidas electrónicas y no gestionado por España. Es vital disponer en el futuro próximo de un sistema alternativo que mejore la robustez frente a posibles ataques que puedan inhabilitar el sistema temporalmente (podría ser el sistema basado en la constelación de Satélites Galileo)

Como se ha dicho anteriormente, los sistemas de armas deben estar conectados a los sistemas de información a través de plataformas de mando y control, dotadas de unos CIS que le permiten integrar la vigilancia, inteligencia y reconocimiento, que permiten al jefe ejercer el mando y control de sus unidades subordinadas, constituyendo una de las piezas claves de los modernos sistemas de gestión de la batalla. Las tecnologías hacia donde evolucionan las expectativas de cara al futuro pueden resumirse en las siguientes:

- Infraestructura de redes y seguridad: SDH, ATM, IP v.6, GBS, WAP, PKI.
- Arquitectura *web* y entornos de aplicación XML y WML.
- Sistemas distribuidos sobre plataformas J2EE.
- Técnicas de compresión de datos.
- Miniaturización de componentes electrónicos con circuitos con substratos multicapa, microondas en 3D, multicapa cerámica TLC (*Low Temperature Cofired Ceramics*).

- Aumento del margen de frecuencias hacia la banda K y superiores (o hacia frecuencias inferiores en comunicaciones con submarinos).

- Proceso digital de señales intensivo mediante DSP (*Digital Signal Processor*) y FPGA (*Field Programmable Gate Arrays*).

- Memorias digitales de radio frecuencia para la realización de técnicas de engaño y perturbación más eficaces.

- Etapas amplificadoras de potencia en estado sólido.

- Nuevos algoritmos de superresolución en radiogoniometría y estimación espectral.

- Enlaces satélite portátiles, fijos y móviles.

- Protocolos OTAN para radio VHF y UHF (*Software Defined Radio*) y HF (pila de protocolos *HF House*).

- Interoperabilidad de redes mediante adopción de protocolos TACOMS Post 2000.

- Enlaces de Datos Tácticos Link 16 y Link 22.

Conclusiones

Hemos visto que la infraestructura del área tecnológica necesaria para gestionar la información debe extenderse desde el más alto escalón de mando hasta el ambiente táctico.

Por lo tanto, las conclusiones a extraer se deberán relacionar con estos dos aspectos, para que, sin solución de continuidad y formando un todo o red de mando y control en la que sus nodos sean totalmente interoperables, se satisfagan las necesidades de gestión de información en las Fuerzas Armadas.

1. Tecnologías a desarrollar ([32]) (en algunos casos, iniciado ya su desarrollo):

[32] MADOC: El Ejército del Futuro. y Manzano García, D. José Carlos. Conferencia, ISDEFE "Capacidad NEC" 2005

- Transporte de datos (Sistemas de Transmisión/enlaces de Datos).
- Gestión de la diseminación de la información (recopilación de la información, optimización en entornos dinámicos, intercambio de información).
- Infraestructura informática distribuida:
  - Dispositivos y componentes electrónicos (procesadores, sistemas de almacenamiento, dispositivos de entrada/salida, etc.).
  - Servicios informáticos en red (correo electrónico, servicios de impresión, etc.).
  - Dispositivos de energía.
- Apoyo al procesado/decisión:
  - Procesos de dar sentido.
  - *Software* de integración de la información (ejemplo fusión y correlación de datos).
  - Razonamiento guiado informáticamente.
  - Agentes *software* cooperativos.
  - Agentes de mediación en lo heterogéneo.
  - *Software* de optimización.
- Interfaz hombre-máquina:
  - Funciones fundamentales.
  - Visualización.
  - Interfaz mediante voz y lenguaje.
  - Agentes explicativos.

  - Agentes de alerta.
  - Agentes para incitar el conocimiento.
  - Interfaces hombre-máquina en el que se tenga las manos disponibles.
  - Entrada/salida en entornos estresantes.
- Aseguramiento de la información y de la seguridad:
  - *Software* y protocolos de seguridad en redes.
  - *Hardware* de seguridad en redes para usuarios móviles.
  - Acceso adaptativo a la información a través de múltiples formas.
  - Detección de intrusos, previsión y respuesta.
  - Detección y respuesta ante amenaza de personas que estén enteradas.
  - Cifrado.
  - Protección y control de accesos físicos a los equipos.
- Integridad de la información:
  - Máquinas para estimaciones y deducciones.
  - Presentación y entendimiento de la integridad.
  - Conciencia e incertidumbre.
- Modelado y simulación rápido y distribuido de análisis “y sí” y de gestión de la información:
  - Algoritmos y procesos probabilísticas robustos.
  - Aprendizaje automatizado.
  - Agentes inteligentes distribuidos.

- Representación de la información:
  - Datos.
  - Metadatos.
  - Arquitecturas.
  - Relaciones semánticas.
  - Sistemas de Información Geográfica (GIS).

2. Redes tácticas:

- La evolución de las redes telecomunicaciones tácticas, hacia un entorno centrado en NCW y el concepto NNEC exigen que las redes tácticas terrestres se integren en la WAN de mando y control y cuenten con un núcleo de red (*backbone*) modular, de gran capacidad (del orden de gbps), síncrono, que funcione de forma análoga a una Intranet IP (IP v.6) con gestión de QoS para vídeo y voz, accesible a través de nodos de acceso con interfaces de radio o de fibra óptica, redundante y tolerante a fallos.

- La interoperabilidad de las comunicaciones tácticas en los próximos años tendrá tres ejes principales de evolución: Los trabajos en materia de modelos de datos para mando y control de la OTAN (desarrollados en el foro MIP (*Multilateral Interoperability Program*), el cambio de paradigma de interoperabilidad hacia NNEC y NCW (incluyendo la publicación y suscripción de servicios Web), así como la implementación de puntos de interoperabilidad conforme a los STANAG de TACOMS pos 2000.

- Las comunicaciones telefónicas se harán mediante VoIP, aprovechando la infraestructura de redes LAN IP (con gestión de la QoS) de los propios puestos de mando y la propia del núcleo de la red táctica terrestre.

- Las comunicaciones radio evolucionarán hacia la adopción de los protocolos OTAN de comunicaciones HF (HF *House*) y de las formas de onda de la radio definida por *software* (SDR) que se vayan normalizando. Se generalizará el

empleo de protocolos de acceso al medio, corrección de errores y medidas EPM (*Electronic Protection Measures*), como salto en frecuencia, y anchos de banda típicos superiores a los actuales (HF hasta 2400 bps brutos, VHF en torno a los 56 Kbps brutos, UHF en torno a 2 Mbps, SHF en torno a 2,5 Gbps brutos y satélite desde 64 Kbps a un máximo de 500 Mbps -INTELSAT- brutos) que permitan garantizar tiempos de transmisión y recepción de datos acotados y el intercambio de información entre sistemas en tiempo real o casi real. Los cada vez más próximos apoyos aéreos y de helicópteros a unidades terrestres exigirán que los sistemas de mando y control táctico incorporen terminales capaces de enlazar mediante Link 16 en tiempo real con plataformas aéreas. Del mismo modo, las cada vez más frecuentes misiones humanitarias que se llevan a cabo en zonas dañadas por catástrofes con pocas infraestructuras aconsejarán la adopción de sistemas de radiotelefonía celular escalable como TETRAPOL y potenciar la capacidad de conectar las redes tácticas terrestres a redes civiles POTS, GSM y GPRS.

- Todo ello precisa de forma imperativa que, previamente a la obtención de los sistemas definitivos, se realicen los demostradores y prototipos que permitan realizar, en estrecha colaboración entre las Fuerzas Armadas y los fabricantes, un proceso iterativo, en espiral, de mejoras sucesivas de manera que se garantice el resultado mejor y más adecuado.

- Todos los esfuerzos, tanto de las Fuerzas Armadas como de la industria, convergen en la misma dirección; y todos los actores de este prometedor e incierto futuro estamos convencidos de nuestra capacidad para vencer las dificultades y de nuestra disposición para lograr los objetivos que el inmenso reto tecnológico que se vislumbra nos permita alcanzar.

Bibliografía

- ALBERTS, David S., GARSTKA, John J. y STEIN, Frederick P. Neetwork Centric Warfare: developing and leveraging information superiority. CCRP Publication series. FEB 2000.
- BARDAJI, Rafael L. La transformación de la defensa: Implicaciones para la industria. GEES, Nov. 2003. http://gees.org/articulo/321
- CODERE, Paul C. The Tactuical Infosphere. GDR 99 Communications System. http://www.global-defence.com/1999/comms. 03.05.06
- JORDAN, Javier y CALVO, José Luis. El nuevo rostro de la guerra. EUNSA . Pamplona, 2005.

- Mc GREGOR, Douglas, PhD, USA Army Transformation: Implications for the Future (Statement). July 2004. http://www.lexingtoninstitute.org
- MADOC. Ejército de Tierra. Campo de batalla futuro. 2005
- MADOC. Ejército de Tierra. El Ejército del Futuro. 2005
- MADOC. Ejército de Tierra. Tendencias. 2005
- MANZANO GARCIA, José Carlos. Conferencia. ISDEFE. "Capacidad NEC". III Curso Superior de Gestión de Programas 2005. DGAM.
- MARTI SEMPERE, Carlos. Tecnología de la defensa. Instituto Universitario "General Gutiérrez Mellado" (UNED) Madrid, 2006
- McKIERNAN, David D. Network Enabled CApabilities Course. Presentación en EDE (Holanda) 23-26 Octubre 2006.
- NATO. NNEC. Feasibility Study. V. 2.0 October 2005
- NATO. NNEC. Vision and Concept. February 2006
- ORDEN DEF/315/2002 de 14 de febrero. Plan Director de Sistemas de Información y Telecomunicaciones
- SUBCIS de JCISAT del Ejército de Tierra. Documentación de la Sección de Ingeniería. Octubre 2006
- KRAMER, Franklin D. y CITTADINO, John C. Sweden`s Use of Comercial Information Technology for Military Applications. Defense Horizons. OCT 2005
- TOOMEY, Christopher J. Army Digitization: Making it Ready for Prime Time Parameters, USA. Winter 2003-2004
- TOOMEY, Christopher J. C4ISR in the Stryker Brigade Combat Teams. Military Review May-June 2003.
- Warfighter Information Nertwork-Tactical (WIN-T). Presentación. http://peoc3t.monmouth.army.mil/WIN-T

CAPÍTULO CUARTO

EL ESFUERZO DE LA INDUSTRIA ESPAÑOLA EN LA INNOVACIÓN DE TECNOLOGÍAS PARA LA GESTIÓN DE LA INFORMACIÓN EN EL CAMPO DE LA DEFENSA

EL ESFUERZO DE LA INDUSTRIA ESPAÑOLA EN LA INNOVACIÓN DE TECNOLOGÍAS PARA LA GESTIÓN DE LA INFORMACIÓN EN EL CAMPO DE LA DEFENSA

Por SILVIA SORIANO ARÉVALO

Introducción

Para posicionar la situación actual de la industria española de defensa es necesario realizar una visión de la situación de la industria americana y europea en la actualidad. De este modo, podremos fijar un marco adecuado para conocer de un modo más realista la situación, así como obtener el papel que juegan las grandes potencias (Estados Unidos y Europa) y su relación con España.

Del mismo modo, es importante destacar el momento de transformación de las Fuerzas Armadas que está teniendo lugar en todo el mundo. Habrá que analizar este proceso, puesto que no se trata de un proceso aislado, sino de un proceso que, aunque originado en el seno de las Fuerzas Armadas estadounidenses a finales de los años noventa y que se aceleró de un modo extraordinario después del los atentados del 11 de septiembre de 2001 (11-S), se ha extendido a todos los países y en la actualidad está siendo una constante de las Fuerzas Armadas española. Esta transformación no pasa inadvertida ante la propia industria, sino que por el contrario alimenta y contribuye a que esa transformación se lleve a cabo.

Es importante resaltar las grandes aportaciones que elInvestigación y Desarrollo (I+D) militar ha hecho a el ámbito civil a nivel mundial. Después de la Segunda Guerra Mundial, la supremacía tecnológica que siempre había acompañado al entorno militar, cedió paso a los avances tecnológicos liderados por el ámbito civil, lo que hizo que las aplicaciones de doble uso, tanto militar como civil, marcaran las tendencias de investigación tecnológica.

La industria de defensa en Estados Unidos

El final de la guerra fría dejó a Estados Unidos con su extraordinario aparato militar afrontando nuevos retos. Las Fuerzas Armadas de Estados Unidos no sólo centraban su atención en la Unión Soviética, sino que además tenía que aceptar un papel multidisciplinar después de un periodo de tiempo relativamente breve. Las nuevas tareas a las que a las que las fuerzas tenían que hacer frente consistían tanto en misiones puramente humanitarias, contando con tropas menores como en misiones de combate con fuerzas extensas por todo el mundo.

Este abanico de tareas en su totalidad cubrió la segunda guerra del Golfo, Somalia, Bosnia, Kósovo, Macedonia, Afganistán e Irak. Podríamos asegurar que desde 1999 hasta la actualidad las Fuerzas Armadas de Estados Unidos han salvaguardado su estatus de gendarme del mundo en el seno del sistema internacional. Dondequiera que se demandara la participación de las fuerzas militares de Estados Unidos, estas debían estar preparadas para hacer frente a cualquier misión. Por otra parte, las Fuerzas Armadas de EEUU sufrieron cambios sustanciales a lo largo de dicho período y desde entonces su mandato ha cambiado de manera drástica. Ya no se trataba de contener a la Unión Soviética ni de una escalada de grandes dimensiones en la fuerza militar, disponiendo de mucho tiempo para ello. Se trataba más bien de de la habilidad de asumir operaciones militares de menor escala que se pudiesen llevar a cabo en localizaciones de interés estratégico para Estados Unidos disponiendo de menos tiempo.

La nueva misión de las Fuerzas Armadas de Estados Unidos requirió una reducción del total de sus fuerzas y también conllevó una reducción del presupuesto de defensa. En el año 1990 las Fuerzas Armadas de Estados Unidos estaban formadas por algo menos de 2,1 billones de efectivos. Diez años después, este número había disminuido aproximadamente un tercio hasta 1,4 billones. Esto ha implicado igualmente una reducción continua del presupuesto destinado a la defensa. A lo largo de esta década, el presupuesto ha sufrido un recorte de alrededor de 100.000 millones de dólares americanos. En el año 1999, el presupuesto de Defensa de Estados Unidos ascendía a 279.000 millones de dólares aproximadamente. Las Fuerzas Armadas estadounidenses se encontraban, tal y como afirmaban los críticos, más o menos en la misma situación que durante la operación *Tormenta del Desierto en* 1991.

Por consiguiente, y no por ello sorprendente, las disponibilidad operativa de las fuerzas se convirtió en una cuestión importante el ámbito de la política de seguridad y de defensa dentro del contexto de la campaña electoral para las elecciones presidenciales del año 2000. Los militares esperaban que la nueva administración Bush iniciara una rigurosa modernización de las Fuerzas Armadas. Básicamente, la visión de una transformación de las Fuerzas Armadas americanas pronostica una:

> "Fuerza futura que se definirá menos por el tamaño y más por la movilidad y la capacidad de reacción, una fuerza más fácil de desplegar y mantener, una fuerza que dependerá más del sigilo, de las armas de precisión y de las tecnologías de la información."

En comparación con Europa, los esfuerzos de Estados Unidos para transformar sus Fuerzas Armadas ya estaban de manifiesto antes del 11-S. Un nuevo y decisivo aspecto, legítimo o no, desencadenado tras los ataques terroristas cobró fuerza en el proceso de transformación de las Fuerzas Armadas estadounidenses, e incluso se obtuvieron más fondos-. A pesar de que ciertos críticos presentes en Estados Unidos argumentan que el propósito subyacente de la transformación, por ejemplo desarrollar sistemas armamentísticos revolucionarios que podrían cambiar completamente la naturaleza tradicional de las Fuerzas Armadas (como podrían ser los vehículos aéreos de combate no tripulados, que a largo plazo sustituirán a los pilotos), apenas recibió la inversión necesaria, la financiación destinada a las plataformas del sistema armamentístico tradicional (aviones de combate, portaviones, tanques de batalla medios), fue extraordinaria.

Las armas que se obtienen hoy en día en Estados Unidos tienen que ser aún más rápidas, más flexibles, más poderosas, menos visibles y de mayor alcance. Los ataques terroristas contra el centro de poder norteamericano, no sólo promueven que las prioridades del secretario de Defensa estadounidense, Donald Rumsfeld, sean la defensa y la seguridad nacionales, sino que además se requiere el desarrollo de las Fuerzas Armadas norteamericanas. Todo esto va dirigido a luchar contra el enemigo número uno de Estados Unidos: el terrorismo internacional. Mientras no existan huellas visibles, Estados Unidos intentarán dar con aquellos que apoyan el terrorismo, haciendo uso para ello de un poder militar arrollador como último recurso aunque no por ello menos importante.

Con el fin de llevar a cabo todas estas transformaciones el presupuesto destinado a defensa y seguridad para el año 2007 alcanzará la cifra de 440 billones de dólares, que se acercan bastante al presupuesto que la administración Reagan destinó a la defensa durante la guerra fría.

Sería de gran interés, destacar en este apartado la importancia que tienen organismos como DARPA (*Defense Advanced Research Projects Agency*) en los avances tecnológicos militares en Estados Unidos. Dicha agencia tiene en marcha una serie de programas que som pioneros en cada uno de sus ámbitos y que darán pie a desarrollo de tecnologías de aplicación de tanta relevancia como en su día hiciera el proyecto Arpanet, financiado por DARPA y que dio lugar a la creación de Internet tal y como lo conocemos hoy en día. En la actualidad, DARPA está liderando varios programas que se pueden clasificar de la siguiente manera:

- Oficina de Programas de Ciencias de la Defensa, que están trabajando en temas tan interesantes como es el de los nuevos materiales y estructuras, en la protección de soldados y vehículos, etc.

- Oficina de Progamas de Tecnología de Procesamiento de la Información, donde se están gestando programas para aumentar el nuevo paradigma de la computación y que se denominará computación de alta productividad, o donde se están creando sistemas capaces de controlar el aprendizaje de *robots*, etc.

- Oficina de Programas de Explotación de la Información, donde se aplica la tecnología más innovadora y vanguardista con el fin de influenciar en las potenciales acciones del adversario para evitar el conflicto, dando forma al escenario de batalla antes de que se produzca el propio conflicto.

- Oficina de Tecnología de Microsistemas, donde son pioneros en la investigación y desarrollo de sistemas o plataformas integradas, basados en tecnologías de electrónica, fotónica, sistemas microelectromecánicos, arqutecturas y algoritmos.

- La Oficina de Programas de Tecnología Estratégica, cuyo principal objetivo es focalizarse en tecnologías que tiene un impacto global amplio y que involucran múltiples servicios como por ejemplo las redes estratégica y tácticas o la seguridad de la información.

- Oficina de Programas de Tecnología Táctica que aplica desarrollos de tecnología avanzada a sistemas militares, enfatizando la aproximación de “sistema militar” como sistemas aeroepaciales y sistemas táctico que proporcionan vigilancia global y participación en operaciones conjuntas. Un ejemplo de programas que seestán desarrollando en esta oficina de programas en es A160, un Vehículo Aéreo no Tripulado (UAV) con un rotor rígido que le permite hacer despegues y aterrizajes en vertical.

La industria de defensa en Europa

Europa posee un potencial enorme, hablando en términos generales. Pero desgraciadamente, los responsables políticos no parecen estar muy dispuestos a hacer uso completo de este potencial. Incluso las tres grandes naciones (Reino Unido, Francia y Alemania), ni son capaces ni parecen estar dispuestas a financiar lo suficiente la seguridad exterior, incluso en contexto actual de guerra internacional contra el terrorismo y de su marcado énfasis en los medios militares. En comparación con Estados Unidos, las tres grandes naciones europeas se están quedando muy atrás, incapaces de igualarse a dicho país con sus 39.000 millones de euros (Reino Unido), 29.000 millones (Francia) y 24.000 millones, (Alemania). Además, no parece haber a la vista ningún gasto record previsto para fines militares que pudiera compensar los enormes esfuerzos hechos por Estados Unidos en este ámbito.

Pero aunque se tiende a comparar la situación a ambos lados del Atlántico, el problema radica precisamente en esas grandes diferencias. Mientras que Estados Unidos siempre ha sido un mercado único con un solo sector industrial, privado y proporcionado a la demanda interna de cada momento, en Europa se han mantenido las industrias nacionales, públicas en la mayoría de los casos, para atender a objetivos estratégicos particulares.

El resultado es que actualmente la Europa -*exceptuando el grupo EADS*-, no representa de hecho ni un mercado ni un sector comunes, sino un conjunto de individualidades que, aunque con capacidad de producción y exportación fuertes en algunos casos, no puede en conjunto competir con Estados Unidos. Como consecuencia de este modelo, la industria europea de defensa presenta numerosas

duplicidades y está muy fragmentada: muchas empresas no tienen el volumen de producción y venta mínimo para sobrevivir; otras lo hacen gracias a las subvenciones gubernamentales más o menos encubiertas a pesar de su falta de competitividad. Un dato importante que confirma esta fragmentación es que a pesar de que Europa destina a defensa aproximadamente la mitad de presupuesto que Estados Unidos, tiene el triple de compañías compitiendo en el mercado, que es también la mitad que el estadounidense.

Se precisa llevar a cabo un proceso para armonizar los requisitos operativos de los distintos ejércitos y coordinar la normativa sobre adquisiciones, especificaciones técnicas, requisitos de calidad y seguridad, como factores que ayudaran a que las empresas estrecharan sus vínculos. Pero el panorama comienza a resultar optimista y algunos cambios que se están produciendo mejoran las perspectivas. Así, la tendencia de la Unión Europea hacia un sistema de defensa a largo plazo, unido a la globalización de los mercados, la moneda única y las economías de escala, llevan a una progresiva pero imparable integración del mercado de defensa.

Dentro de ese marco de armonización e impulsión de colaboración internacional del entorno de defensa han aparecido una serie de catalizadores que están contribuyendo notablemente a que la situación mejore sensiblemente.

Analizando los mismos desde una perspectiva histórica hay que comenzar hablando de Grupo de Armamentos de la Europa Occidental (GAEO). En el año 1976, los ministros de Defensa de la Organización del Tratado del Atlántico Norte (OTAN), con excepción de Islandia, crearon el Grupo Europeo Independiente de Programas (GEIP), encargado de estudiar las posibilidades de cooperación en el ámbito del armamento. En el año 1992, este pasó a denominarse GAEO. En su seno se han desarrollado iniciativas como el Programa EUCLID de cooperación tecnológica.

Hay que mencionar también al Grupo Europeo de Industrias de Defensa (EDIG), como asociación de asociaciones industriales europeas del ámbito de la defensa que agrupa a todos los países miembros del GAEO.

La OTAN, por su parte, y trascendiendo ya al ámbito puramente europeo, dispone también de instrumentos para articular la cooperación, como son la Conferencia de

Directores Nacionales de Armamento (CNAD) en un plano oficial, y el Grupo Industrial Asesor de la OTAN (NIAG) en el ámbito industrial.

Han existido y existen muchos otros foros y grupos que no enumeramos, y todos ellos se fijaron como meta a la creación de una Europa unida en la esfera de la defensa y la seguridad, tratando de alcanzar este objetivo desde distintos enfoques, siempre complementarios y no excluyentes.

Quizás deben analizarse con mayor detalle tres de ellos: la Carta de Intenciones (LOI), la Organización Conjunta de Cooperación en Material de Armamentos (OCCAR) y la Agencia Europea de Defensa (EDA) que apenas acaba de completar su primer año de existencia.

Estas tres iniciativas convergen hacia un doble objetivo, consolidar la oferta, por un lado, y concentrar la demanda, por otro. La consolidación de la oferta, por imperativo de la competitividad, se pretende articular creando un marco jurídico que facilite las actividades de las empresas europea de defensa en diversas áreas. La concentración de la demanda, por su parte, trata de satisfacer la necesidad de contratación con una gestión unificada de los grandes proyectos que permita la rentabilidad de una economía de escala y la racionalización de la planificación a largo plazo.

La LOI

La LOI fue firmada el 6 de julio de 1998 por los ministros de Defensa de Alemania, España, Francia, Italia, Reino Unido y Suecia, y tiene su antecedente más inmediato en la Declaración Conjunta de los Ministros de Defensa de esos cinco países, en abril del mismo año, en la cual reflexionaban sobre la necesidad de una industria fuerte, como elemento clave para la formación de Europa, también en el ámbito de la defensa y la seguridad común. Suecia se adhirió posteriormente, conformándose el grupo de seis componentes.

La LOI se apoya en dos pilares: la existencia de una industria de Defensa competente y eficiente, base del desarrollo tecnológico europeo, y un decidido apoyo por parte de los gobiernos a la creación de una industria única, a través de la armonización de normas y requisitos. Es decir, la LOI no pretende fijar el camino

para la reestructuración industrial, sino allanar este camino para que sean las propias empresas quienes lo recorran con el menor número de obstáculos posible.

Esta LOI fue elevada a rango de Tratado Internacional, mediante el acuerdo-marco firmado el 27 de julio de 2000 por los países firmantes de la LOI, entrando en vigor en España, tras su ratificación por el Parlamento, el 11 de agosto de ese mismo año. El acuerdo-marco, si bien trata, básicamente, las mismas áreas que la LOI, supera el carácter no vinculante de esta, diseñando el marco político y jurídico para facilitar la reestructuración industrial.

Son seis las áreas de actuación de la LOI:

1. *Seguridad de suministros.* En este área, y partiendo de la premisa de que una de las consecuencias probables de la reestructuración de la industria de defensa sea la aparición de las denominadas Empresas Transnacionales de Defensa (ETD) y el posible abandono de la capacidad industrial nacional, con la aceptación de la dependencia recíproca, se pretende garantizar la seguridad del suministro de productos y servicios de Defensa entre las partes firmantes.

   Esta seguridad se articula tanto para tiempos de paz, mediante calendarios negociados con arreglo a las prácticas comerciales nacionales, como para momentos de emergencia, crisis o conflicto armado con la aplicación de los principio de prioridad y restitución.

2. *Procedimientos de transferencia y explotación.* Hay que distinguir entre los movimientos de productos y servicios entre las partes, denominadas “transferencias”, y las exportaciones de estas a terceros estados no firmantes de la LOI/acuerdo-marco. Respecto a las primeras se distinguen a su vez en:

   - Las transferencias realizadas en el marco de un programa cooperativo, que se pretenden simplificar con la creación de la licencia global de proyecto.

   - Las transferencias realizadas fuera de dicho marco, en las que los objetivos son armonizar los procedimientos de concesión de licencias y reducir los requisitos administrativos.

Por su parte, en el caso de las exportaciones a terceros, cuando se encuadran en un programa cooperativo, se aspira a que los países LOI participantes acuerden, mediante consenso, tanto los principios que las rijan, como los procedimientos a seguir, y fundamentalmente los destinos de las mismas, y en aquellas que se produzcan fuera de esos programas, que se gestiones de conformidad con el Código de Conducta de la Unión Europea.

3. *Seguridad de la información.* En este ámbito, se aboga por conjugar, la seguridad de la información clasificada con el fomento de la cooperación industrial, mediante una armonización de los procedimientos relativos a las habilitaciones de seguridad, transmisión de información clasificada y visitas, todo ello regido por el principio de las necesidad de conocer (*need to know principle*).

4. *Investigación y tecnología.* Se impulsa la cooperación en este campo, al facilitar el intercambio de información en Investigación y Tecnología (I+T) entre países, evitando duplicidades y optimizando los recursos limitados destinados a I+T. Al mismo tiempo, se pretenden fijar políticas y procedimientos comunes para el desarrollo de programas conjuntos.

5. *Tratamiento de la información técnica.* Se refiere principalmente a la armonización y simplificación de las transferencias de la información técnica, mediante una normativa consensuada que reduzca las restricciones relativas al tratamiento, divulgación y uso de dicha información.

6. *Armonización de requisitos militares.* Esta es un área fundamental, ya que los países LOI/acuerdo-marco reconocen que para afrontar las futuras exigencias de seguridad y defensa deberán ser capaces de operar conjuntamente o como parte de una coalición, y para ello deben armonizarse las exigencias militares de sus Fuerzas Armadas y los procedimientos de adquisición. A tal fin, se señala la necesidad de establecer una metodología que mejore la coordinación para definir los requisitos militares necesarios, especificar los sistemas en los que estos deban traducirse, planificar las inversiones necesarias, y mantener un diálogo común con la industria de defensa.

La OCCAR

La OCCAR puede ser considerada como el principal elemento de cooperación industrial en Europa. Sus orígenes se remontan a un acuerdo establecido entre Francia y Alemania en el año 1993 para crear una estructura que unificara las normativas entre ambos países y facilitara la gestión de programas conjuntos. En 1996, Italia y Reino Unido se unen a esta estructura, dotándola de personalidad jurídica en 1998. En la actualidad, la OCCAR cuenta con una oficina permanente en Bonn.

Los principios básicos que rigen este organismo son cuatro:

- La cooperación entre los Estados miembros para reforzar la industria europea de defensa.
- La consolidación y el desarrollo de una base industrial y tecnológica europea.
- El abandono del “justo retorno” programa a programa, que se sustituye por el concepto de “retorno económico global”.
- El trato preferente a los desarrollo s de los países OCCAR.

Para alcanzar estos objetivos, se realizan una serie de actividades como:

- Gestión de programas de cooperación, incluyendo el control de la configuración y apoyo en servicios y actividades de I+D.
- Gestión de programas nacionales de los países miembros que le sean asignados.
- Elaboración de especificaciones comunes para el desarrollo y adquisición de equipos definidos conjuntamente.
- Coordinación y planificación de actividades conjuntas de I+D y estudios técnicos, destinados a satisfacer futuros requerimientos.
- Coordinación de las decisiones nacionales para disponer de un tejido industrial y tecnológico común.
- Coordinación de las inversiones y del uso de las instalaciones.

La OCCAR permite la incorporación de otros países que acepten tanto sus principios básicos como el proceso de toma de decisiones por mayoría cualificada reforzada. Esta última supone que no podrán adoptarse decisiones con una oposición igual o superior a diez votos, en otras palabras que no se aprobará ninguna decisión que cuente con la oposición de al menos uno de los cuatro estados fundadores, ya que estos se han otorgado diez votos cada uno.

En la actualidad, la OCCAR cuenta con seis países como Estados miembros: Alemania, Francia, Italia, Reino Unido, Bélgica y España. España, fue el último país en incorporarse y lo hizo en enero de 2005, iniciando su andadura en dicha organización con la participación en los Programas A-400M y *Tigre*.

Los siete programas que se están gestionando desde las OCCAR a día de hoy son:

1. *A-400M.* Este Programa surgió de la necesidad de que en el panorama actual de las Fuerzas Armadas, se requieren medios cada ves más flexibles y de menor coste, capaces de desplazar recursos de forma rápida y eficaz. Hasta la fecha está prevista la contrtación de 180 unidades repartidas en tre los diferentes países implicados en el programa: Alemania, Bélgica, España, Francia, Luxemburgo, Reino Unido y Turquía.

2. *Boxer.* Alemania y Holanda son los socios tecnológicos para el desarrollo del boxer, una nueva plataforma acorazada de las denominadas 8 por 8. El nuevo concepto de tener dos compartimentos separados e independientes, por un lado el compartimento de conducción (desde el que se conduce el vehículo), y por otro lado un “módulo de misión” que se puede reutilizar de diferente modo dependiendo del objetivo de la misión, hacen del Boxer un vehículo altamente flexible y adaptable al entorno y a la situación para la que está siendo utilizado.

3. *COBRA.* Es el acrónimo de (*Counter Battery Radar*) que se trata de un trabajo conjunto entre Alemania, Francia y Reino Unido, para el desarrollo de un radar de largo alcance. En la actualidad COBRA, es considerado uno de los radares de posicionamiento de armas más avanzado del mundo.

4. *FREMM.* Es el Programa más innovador y ambicioso de la industria naval europea de defensa. Este programa está coordinado por Francia e Italia con el

objetivo de construir fragatas que puedan adquirir un potencial más diverso del que ha venido siendo hasta ahora propio de las fragatas. De modo, que sean capaces de adaptarse a los nuevos entornos de operaciones que demanda la situaciones militares actuales.

5. *FSAF.* Es el nuevo sistema antimisiles de superficie-aire en el que está trabajando la industria europea. Nuevamente se tiene como objetivo impulsar tecnologías totalmente novedosas en el ámbito de los nuevos sistemas de armas antimisiles. Existen dos fases de este programa, en la primera de ellas colaboran Italia y Francia, y contando con la colboración del Reino Unido en la segunda.

6. *ROLAND.* Es un sistema antimisiles que lleva en el mercado de defensa desde 1978 y sigue en uso en Francia y Alemania. Lo que la OCCAR gestiona dentro de este programa es el mantenimiento del sistema y la evolución tecnológica del mismo. Aunque su futuro en Francia resulta un poco incierto.

7. *Tigre.* El Programa *Tigre* está diseñado para cubrir un gran rango de misiones demandadas para helicóptero. En el año 1988, Francia y Alemania firmaron un acuerdo para el desarrollo de este nuevo helicóptero, del que pronto se completaron dos versiones. La versión francesa será adquirida por el Ministerio de Defensa francés y el español. Y en total dentro del programa se ha firmado un contrato inicial para un suministro de 160 helicópteros para todos los países implicados en el program que a día de hoy son: Francia, Alemania y España.

La EDA

La EDA se formó en julio de 2004 con bajo el amparo de la Unión Europea y con el objetivo único de construir las capacidades necesarias para una Europa más segura.

La Agencia está diseñada para “ayudar a los Estados miembros en sus esfuerzos por mejorar las capacidades europeas de defensa en la gestión de crisis”. Más específicamente esos objetivos se pueden enumerar del siguiente modo:

- Desarrollo de capacidades de defensa.

- Cooperación armamentística.

- La defensa europea, base tecnológica e industrial y mercado de equipamiento de defensa

- I+T.

Para el año 2007, en el plan de trabajo que la EDA acaba de aprobar el pasado 13 de noviembre de 2006, se enumeran las siguientes iniciativas como áreas prioritarias:

- C3: aumentar el contexto de trabajo en NNEC (*Network Enabled Capabilities*) elaborando una hoja de ruta más allá del 2010 de lo que se podría denominar "concepto NNEC de la Unión Europea" conjuntamente con otros actores europeos y ayudando en la definición o elaboración de los requisitos de intercambio de información. Continuar los esfuerzos en las comunicaciones mediante satélite, para una mejor coordinación en una cooperación a corto plazo.

- Inteligencia: trabajar más profundamente en los sistemas de Inteligencia, Vigilancia y Reconocimiento (ISR), así como en la interoperabilidad de los mismos. Implementar el proyecto de la Estación de Explotación de Imagen Táctica (TIES) y desarrollar el proyecto de la Herramienta de Análisis de Inteligencia Universal (UIAT).

- CBRN: impulsar los esfuerzos en detección e identificación de amenazas de tipo, químico, radiológico, nuclear y bacteriológico.

- Vigilancia marítima: continuar trabajando en las tres áreas clave, como son las comunicaciones, los UAV (aviones no tripulados) tácticos e identificación de objetivos pequeños.

- UAV: gran esfuerzo por apoyar programas emergentes de UAV, así como para las tecnologías y los sistemas asociados.

En definitiva, las tres iniciativas analizadas- LOI/acuerdo-marco, OCCAR y EDA, se muestran como dos instrumentos eficaces para llevar a cabo la reestructuración de la industria de defensa europea, pero su andadura no estará exenta de dificultades y riesgos.

No son pocas las voces que han advertido del riesgo de producirse una integración en dos escalas, con países de primer nivel, que asumirán el papel de contratistas principales, llevando el peso de los grandes proyectos y aumentando aun más su capacidad tecnológica e industrial, y otros de segundo nivel, menos suministradores y mantenedores de los anteriores. Así, la distancia entre ambos grupos en lugar de disminuir, irá aumentando.

Para que esto no suceda, es imprescindible que exista voluntad política, en las naciones con una industria más sofisticada, de favorecer la participación del mayor número posible de Estados en programas de cooperación tecnológica, fomentando el desarrollo de las áreas de excelencia de todos los países, independientemente de su poderío industrial.

Se requiere también, para evitar una industria de defensa europea de dos niveles, una alta dosis de generosidad en la industria de los países más desarrollados. Estos deben tener en cuenta no tanto los efectos inmediatos de las posibles cesiones hacia los menos avanzados, como el horizonte de una integración que favorecerá a todos. Porque del mismo modo que nadie discute la necesidad de los grandes, tampoco puede ponerse en cuestión a pequeños y medianos, base de cualquier industria. De otro modo, estaríamos alimentando la creación de un gigante con pies de barro, incapaz de resistir los embates de los competidores extranjeros.

Por su parte, la actividad política a nivel nacional, se ha desarrollado de manera distinta de cada uno de los países, destacándose la política de privatizaciones que supone un cambio de orientación. La privatización de las empresas de defensa, no sólo se ha limitado a una simple venta de las acciones de la iniciativa privada, sino que además, ha supuesto un giro a la concepción de su naturaleza. Estas empresa fueron creadas bajo titularidad pública por motivos estratégicos y de seguridad nacional, y sus resultados económicos quedaron subordinados a dichos motivos. Se pretendía, más que la rentabilidad económica, la seguridad en el suministro de los productos de defensa, que en una eventual dependencia del exterior no se podría garantizar.

Sin embargo, esta autarquía industrial se ha revelado inviable en un contexto de globalización económica y de integración europea, puesto que, por una parte la

competitividad exige la creación de productos de un alto nivel tecnológico, cuyo desarrollo conlleva un elevado coste financiero difícil de asumir por un estado en solitario, y por otro, las necesidades presupuestarias derivadas de la contención del déficit público impiden asumir dichas pérdidas. De esta forma la política de privatizaciones ha permitido a muchas empresas regirse por criterios de rentabilidad, lo que además hará que se creen productos competitivos en el mercado.

En definitiva, los gobiernos, tanto a escala europea como nacional, han diseñando un escenario, no exento de dificultades, en el que la industria de defensa puede actuar con criterios racionales y de rentabilidad, y en el que al mismo tiempo, este juego de mercado permita crear los instrumentos necesarios que garanticen, nos solo la seguridad de las naciones que integran la Unión Europea, sino además, la capacidad de actuación autónoma de la misma como actor estratégico internacional.

Partiendo de este escenario, es claro que el campo empresarial afronta la excesiva fragmentación, sobrecapacidad productiva y la falta de coordinación del sector, de la mano de dos procesos fundamentales:

- Concentración en el ámbito nacional.

- Integración en grupos transnacionales.

El primero de los procesos, la concentración de empresa del sector, trata de resolver su histórico sobredimensionamiento, y se está llevando a cabo mediante un proceso de fusiones empresariales de tipo vertical y horizontal. Desde una perspectiva general puede señalarse que la primera modalidad ha sido utilizada por aquellas empresas integradoras de sistemas de combate que, a fin de ganar escala y abordar de forma coordinada los grandes proyectos de I+D que demanda el mercado, se han fusionado con sus principales suministradores de subsistemas. Las fusiones horizontales, por su parte, se han producido entre empresas que competían en un mismo subsector, y han traído consigo no solo una mayor escala de las nuevas empresas resultantes, sino, por un lado una mayor racionalización en la oferta de productos al mercado, y por otro una unificación de la disparidad de modelos existentes así como una interoperabilidad entre los mismos.

En sintonía con estos movimientos nacionales y adaptándose a la nueva escala global de economía, se ha venido desarrollando un segundo proceso caracterizado por la integración de esas empresas en grupos multinacionales. En este proceso pueden distinguirse, a su vez varias modalidades que van desde la integración, por venta de la empresa a una gran multinacional, pasando por la incorporación a un grupo internacional de empresas y la creación de nuevos grupos *ad hoc*.

Concluyendo y antes de abordar la situación española, las empresas de defensa ante el cambio del panorama político-estratégico y en un contexto de economía globalizada, afrontan el desafío de la reestructuración de su sector presentando líneas de actuación flexibles y adaptables, tales como alianzas, fusiones o adquisiciones, destinadas bien a crear grupos dominantes de cara al mercado interior, o bien como preparación para otros mercados y con una especialización y concentración de actividades en mercados que se dominan, evitando la dispersión.

La industria de defensa en España

España no se ha mantenido ajena a todo el escenario general descrito hasta el momento. Por el contrario, las iniciativas políticas y empresariales se han mostrado, en general, en consonancia con el mismo.

En el ámbito político, se ha apostado tanto por un proceso de privatización y como por una integración de nuestro país en los acuerdos y organizaciones europeas. Estas líneas de acción política han favorecido que desde la industria se desarrollen estrategias de concentración, mediante fusiones horizontales y verticales, y de integración en grandes grupos transnacionales, como ha ocurrido en la mayoría de países europeos. Sin embargo, la posición española es más compleja de lo que podría deducirse en un principio. Esta complejidad se deriva, en primer lugar, de su posición intermedia entre los grandes productores de material de defensa y los meros compradores y, en segundo lugar, por la apuesta por hacer compatible la autonomía estratégica europea con el mantenimiento del denominado “vínculo trasatlántico”.

Respecto de lo primero, la integración en una industria europea de defensa, el sector español ha mostrado su preocupación por que ésta no se realice empleando como única fórmula la incorporación a grandes grupos transnacionales, o relegando a las

pequeñas y medianas empresas al mero papel de montadores de sistemas de armas. No existe un modelo único de integración, y España debe analizar las ventajas e inconvenientes caso a caso, modulando su actuación en función de las características de cada subsector, y poniendo especial énfasis en el acceso no sólo a los Programas de I+D en curso, sino a aquellos que en el futuro marcarán la capacidad de nuestra industria.

En cuanto a lo segundo, España debe ser consciente de que la pretendida autonomía estratégica europea tienen que asentarse en una reestructuración de la industria de defensa, pero al mismo tiempo, dicha autonomía no puede conducir a un aislamiento frente a Estados Unidos. Si bien es cierto que, en el terreno económico y en un contexto de globalización, Europa debe reforzar su competitividad industrial, no es menos cierto que el propio contexto económico y tecnológico demanda la colaboración y cooperación con Estados Unidos.

España debe seguir haciendo compatibles tres factores que determinan su posición:

- La creación de una industria de defensa competitivamente fuerte y tecnológicamente avanzada, que permita a la Unión Europea dotarse de las capacidades militares que su peso como actor internacional exige.

- Mantener y profundizar las relaciones con Estados Unidos y también con Iberoamérica y los países del Mediterráneo.

- La defensa de sus intereses industriales que garantice no ya la mera supervivencia de su tejido industrial, sino la creación de polos de excelencia que permitan estar a la vanguardia de los avances tecnológicos.

Organizaciones nacionales para la activación

de la industria de defensa

En un panorama nacional como el nuestro, tan atomizado en lo que a la existencia de industrias de defensa se refiere, se han creado una serie de foros y organizaciones que favorecen el aumento de rentabilidad de dichas industrias:

1. *AFARMADE.* Es la Asociación Española de Fabricantes de Armamento y Material de Defensa y Seguridad y se define como una asociación profesional, privada, de

carácter empresarial, sin ánimo de lucro, que tiene por objeto la defensa y fomento de los intereses comunes de los fabricantes españoles de armamento y material de defensa y seguridad.

AFARMADE goza de personalidad jurídica propia, independiente de la de sus miembros, y cuenta con la capacidad de obrar necesaria para el cumplimiento de sus fines, pudiendo ser titular de derechos y obligaciones de toda clase y realizar, en general, todas las actuaciones apropiadas para alcanzar sus objetivos, tanto en España como en el extranjero.

AFARMADE tiene por objeto fomentar el adecuado desarrollo del Sector de fabricantes de armamento y material para la Defensa y la Seguridad considerándolo como un todo, y colaborar en la defensa de sus intereses específicos, por lo que dedicará su actividad a cuantas cuestiones afecten a su desarrollo y especialmente en lo relativo a:

- Representación de las empresas del sector ante la Administración y ante los diferentes organismos nacionales e internacionales.
- Defensa de los intereses comunes de la Industria.
- Promoción de la colaboración entre industrias.
- Promoción del sector español de defensa y seguridad.
- Realización de diversos estudios, informes y catálogos, así como organización de conferencias y cursos de interés, relativos al ámbito de la defensa y seguridad.
- Desarrollo de acciones encaminadas a crear una imagen positiva del sector.

2. *Fundación Círculo de Tecnologías para la Defensa y la Seguridad.* Esta fundación se constituye el pasado 11 de mayo de 2006 c*omo foro d*e encuentro y debate entre la Administración, las Fuerzas Armadas y de Seguridad del Estado, la Universidad, los centros de investigación y las empresas de los sectores de seguridad y defensa. Uno de sus fines es el de potenciar un clima de mutua confianza y colaboración entre los agentes de los citados sectores y contribuir a

un mayor intercambio de información y conocimientos entre todos los profesionales relacionados, en general, con las tecnologías avanzadas de aplicación en defensa y seguridad y, especialmente, con las Tecnologías de la Información y las Comunicaciones.

Los fundadores de esta institución son la Fundación General de la Universidad Politécnica de Madrid, el Colegio Oficial de Ingenieros de Armamento, la Sociedad de Sistemas para la Defensa de España (ISDEFE) y el Grupo Tecnológico Industrial GMV. S. A.

La Fundación es la heredera del Círculo de Tecnologías para la Defensa y la Seguridad, una entidad encuadrada en la Fundación Universidad Empresa (FUE) que nació en el año 1983 con ocasión de las I Jornadas de Electrónica Militar, organizadas por la FUE. Ese mismo año se creó el Círculo de Electrónica Militar. Posteriormente, en 1998 pasó a denominarse Círculo de Tecnologías para las Defensa y en el año 2001 Círculo de Tecnologías para la defensa y la seguridad.

Entre los objetivos principales de la fundación Círculo cabe destacar:

- Fomentar iniciativas que tiendan a la creación y al desarrollo de una tecnología nacional de aplicación a la defensa y la seguridad, especialmente en las áreas de electrónica, informática y comunicaciones.

- Actuar de catalizador en las relaciones entre personas, organismos, instituciones y empresas que tienen intereses y realizan actividades dentro del sector de la defensa y la seguridad.

- Facilitar a los asociados una permanente actualización de las tecnologías para la defensa y la seguridad a través de actividades de formación, investigación y desarrollo.

- En el mercado nacional de la industria de defensa se puede una clasificación por sectores donde quedarían englobadas todas las empresas del ámbito de defensa:

    - Sector aerespacial.

- Sector de munición y armamento.
- Plataformas Navales.
- Electrónica.
- Ingeniería e I+D.
- Material de seguridad.

En todos los sectores anteriormente mencionados, existe presencia de empresas nacionales y que ya han alcanzado una estructura multinacional con representación en muchos países, pero también existen otras muchas compañias multinacionales con presencia en España con un gran potencial tecnológico.

Desafíos presentes y futuros en tecnología

de la información en el ámbito de la defensa

El objetivo de este capítulo es analizar el presente y el futuro de la tecnología de la información aplicada al ámbito de defensa.

Analizando la situación actual descubrimos que uno de los grandes retos a los que nos enfrentamos en la organización militar ya sea en época de paz o en situación de conflicto es el de el colaboración. Como ya hemos comentado en varios apartados a los largo de esta *Monografía*, nos encontramos en la denominada era de la información y hemos dejado atrás la llamada era de la industrialización. Las organizaciones con más beneficios no son aquéllas que más capacidad industrial poseen sino aquellas que tienen más información y que son capaces de extraer el mayor grado de conocimiento de la misma. Toda esta situación es extensible a la problemática que vive defensa en la actualidad, y es de todos conocido que más allá de las capacidades de las que se dispone en todos los órganos del ministerio de defensa (órgano central, Estado Mayor de la Defensa, Ejército de Tierra, Ejército del Aire y Armada), existe una necesidad básica de disponer de la información necesaria cuando y donde se requiera.

Todo este proceso, pasa por seguir colaborando entre agencias como se hace hasta ahora, con el objetivo principal de que la información esté disponible y pueda compartirse entre diferentes organismos y departamentos del Ministerio de Defensa. Afortunadamente, este proceso ya ha comenzado a abordarse y poco a poco se va imponiendo la tendencia de trabajo en entornos colaborativos, haciendo que los sistemas de información puedan facilitar el trabajo en dicho ámbitos. Obviamente, el reto en el futuro, en términos de colaboración, pasa por poder compartir información entre diferentes fuerzas multinacionales.

Otro de los factores clave para poder mantener un sistema de información sólido y robusto es el de las redes de información. Resulta imprescindible asegurar que la información a la que estamos accediendo es la información más actualizada, que no hay errores en los datos y que, por tanto, podemos fiarnos de ese sistema para poder obtener un conocimiento actual de la situación. Para ello, necesitamos crear una red propia, en primer lugar de datos, que es la fuente principal de información y que en última instancia debería convertirse en una red en la que la información pueda fluir de forma segura y fiable entre los diferentes niveles de la organización. Llegando a convertirse en una condición sin equa non para el apoyo a la decisión. Esta metodología es un reto a abordar en el futuro y que cuenta con mucha oposición de la propia organización multinacional, ya que la mayoría de los países son muy sensibles a compartir su información con organismos pertenecientes a otros países.

Todavía estamos relativamente lejos de la situación anteriormente descrita, ya que en la actualidad disponemos de datos y sistemas aislados que operan de forma independiente y que utilizan el concepto tradicional de informática como servicio de los mismos. Ya hay experiencias en otros países, así como en determinados organismos del Ministerio de Defensa como es la Inspección General CIS, que abogan por una aproximación diferente, resaltando la importancia de la información como recurso estratégico de las organizaciones. Este argumento es el que nos lleva a evitar el término informática para denominar a los sistemas de información o tecnología de información. Debe quedar claro que los sistemas de información son la clave para acceder al conocimiento.

La interoperabilidad de los sistemas de información es un requisito imprescindible para poder desligarse del aislamiento de sistemas que existe hoy en día. Para garantizar entornos interoperables ya existen tendencias y estándares tecnológicos: TC/IP, XML, HTML, etc. Por otra parte, la propia OTAN ha contribuido a solventar el problema de interoperabilidad definiendo los stanag. Además los sistemas de información tienen que ser interoperativos, que tienen que servir en entornos y situaciones de trabajo comunes. Un aspecto más a considerar, es aplicar tecnologías basadas en COTS (*Cost of the Shelfs*) y en estándares abiertos, en lugar de utilizar sistemas propietarios y *ad hoc*, técnicamente denominados *legacy*. Aunque inicialmente estas aplicaciones desarrolladas a medida puedan parecer más económicas tienen un elevado coste de mantenimiento tanto correctivo como evolutivo.

Una idea para poder afrontar los retos del acceso al conocimiento mediante el uso de los sistemas de información como herramienta, pasa por la llamada Transformación de las Fuerzas Armadas. Muchos son los países que han abordado esta problemática creando oficinas de transformación en sus ministerios de defensa. En el caso del Ministerio de Defensa español, desde el año 2002 con la creación del Plan Director CIS se intentó resolver este problema, si bien a fecha de hoy no se han producido los cambios organizativos adecuados para llevarlos a cabo en su máxima extensión. Es necesaria una adecuación de la tecnología al ámbito de lo funcional y no de lo orgánico. Lo más relevante es la función, proceso y no quien la realiza. En el futuro lo realmente importante es conocer los procesos de negocio de la organización militar y, tan sólo con el uso de las tecnologías de la información se podrán optimizar esos procesos.

Como hemos visto, lo importante son los procesos, y que el uso de la tecnología es imprescindible para el diseño, gestión y optimización de los mismos, por lo tanto los responsables funcionales así como los de tecnología van a pasar un papel mucho más relevante en la organización en un futuro próximo.

Todas estas ideas fuerza que se han planteado hasta ahora de alguna u otra forma no se han implantado hasta ahora. Es obvio que las tecnologías dan soluciones a cualquiera de las cuestiones planteadas, por lo tanto debe entenderse que si no se

han llevado a cabo es por problemas organizativos o más bien de cultura organizacional.

Este problema no sólo se manifiesta en estamentos militares y civiles de la defensa, sino que las empresas tampoco han asumido ese cambio de paradigma. La rentabilidad a corto plazo y la cuenta de resultados impiden un visión estratégica de estos cambios. Del mismo modo, tenemos que luchar por hacer desaparecer la imagen de relación cliente- proveedor y transformarla en una relación, de al menos, socios tecnológicos encaminadas al modelo *win to win*.

Estamos viviendo una revolución en el mundo de la tecnología, evolucionando de la era de los datos, en la que las decisiones se basan en modelos empíricos y en experiencias anteriores, para llegar a la era del conocimiento, pieza clave en la correcta toma de decisiones en los tres niveles de decisión: estratégico, táctico y operativo.

Dentro de todas estas transformaciones, y como ya se ha mencionado anteriormente, la información adquiere una relevancia clave, convirtiéndose en un recurso estratégico de la organización y, por lo tanto pasa a ser un bien intangible a proteger. Por este motivo, la seguridad de la información también adquiere un gran protagonismo. Durante el último año se han producido varios hitos importantes en torno a esta cuestión: la puesta en marcha de la Infraestructura de Clave Pública del Ministerio de Defensa, la tarjeta inteligente como soporte de la misma y, sobre todo, la elaboración del marco legislativo sobre seguridad de la información. Hay que reseñar que se ha dado la máxima importancia a la seguridad de la información, haciendo recaer la máxima responsabilidad en el secretario de estado de Defensa.

Como cualquier otro recurso de las organizaciones modernas, la información necesita herramientas de gestión que garanticen que esta sea la más adecuada, la última disponible, esté correctamente estructurada y presentada y pueda ser utilizada por quien corresponda y cuando se necesite. Además, esas herramientas de gestión tendrán que posibilitar la anticipación de resultados antes de que estos se produzcan. Las últimas herramientas de modelización de sistemas expertos, minería de datos, etc., utilizan estas técnicas y en futuro cercano se harán imprescindibles

en el apoyo a la toma de decisiones así como en la retrointerpretación de los resultados. En última instancia, dotar de inteligencia a los sistemas.

Históricamente un aspecto, nada baladí, ha sido el coste de estos sistemas. En este ámbito también se está produciendo una auténtica revolución, no sólo por el abaratamiento relativo de los mismo, hoy hacemos más con menos, sino en el propio concepto económico. Se ha pasado de hablar simplemente de gasto en el pasado a su inversión y retorno en el presente, y llegaremos en un futuro próximo de coste-oportunidad, cuánto nos hubiera costado sino hubiéramos realizado las inversiones necesarias.

Conclusiones

La colaboración entre diferentes organismos del Ministerio de Defensa va a ser imprescindible.

En un futuro cercano el flujo de información será transversal y por tanto requerirá ser compartida y utilizada por quien realmente la necesite.

La organización deberá definir sus procesos de negocio y se hará uso de las tecnología para optimizarlos. Por lo tanto, la tecnología será un instrumento y no un fin en sí mismo.

Las organizaciones necesitan un importante cambio cultural para adaptarse a la nueva situación.

Las empresas tecnológicas y proveedoras de tecnología necesitan una adaptación interna a la nueva situación.

Se está pasando del mundo de los datos al de la información, de esta al conocimiento y, a través de esta, a la correcta toma de decisiones tanto en el ámbito estratégico, táctico y operacional.

El nuevo paradigma de la transformación necesita de las tecnologías para ser llevado a cabo.

La interoperabilidad será un aspecto fundamental en el futuro.

La seguridad en la información tomará un carácter predominante en la organización.

Se ha pasado del gasto a la inversión y su retorno y en el futuro hablaremos de coste-oportunidad.

Bibliografía

Plan Director de Sistemas y Comunicaciones. 14 Abril 2002.
Network Centric Warefare. David S. Alberts. 1999.
Fondos Documentales de la Dirección General de Armamento y Material.
Fondos documentales de la Inspección General CIS.
Monografías del CESEDEN
Documento de trabajo. “El desequilibrio de las capacidades militares transatlánticas y el futuro de las relaciones entre EEUU y Europa”. Real Instituto Elcano de Estudios Internacionales y Estratégicos. 2003.
Documentos VII Master de Seguridad y defensa. 2001.
Website de la Agencia Europea de Defensa:Http://www.eda.europa.eu
Website de la oficina de transformación del DoD: http://www.defenselink.mil/transformation/
Website de la OCCAR: http://www.occar-ea.org/
Website de NCOIC (Network Centric Operations Industry Consortium): http://www.ncoic.org/home
Website de DARPA: http://www.darpa.mil

CAPÍTULO QUINTO

LA GESTIÓN TECNOLÓGICA EN LAS FUERZAS ARMADAS: UN FACTOR CLAVE EN LA MEJORA DE SU CAPACIDAD OPERATIVA Y EN LA OPTIMIZACIÓN DE INVERSIONES

LA GESTIÓN TECNOLÓGICA EN LAS FUERZAS ARMADAS: UN FACTOR CLAVE EN LA MEJORA DE SU CAPACIDAD OPERATIVA Y EN LA OPTIMIZACIÓN DE INVERSIONES

Por CLEMENTINA BRAVO PÉREZ

La necesidad de realizar una gestión tecnológica

Actualmente, uno de los más importantes objetivos de las Fuerzas Armadas de las naciones es la superioridad tecnológica. Las nuevas misiones, y en particular la amenaza del terrorismo, requieren capacidades de anticipación y respuesta que sólo una continua innovación tecnológica puede garantizar. Pero obtener e insertar tecnología es complejo, y más hacerlo con un coste asumible.

Los procesos de transformación que los países avanzados tienen en marcha no se limitan a un redimensionamiento de la fuerza, sino que inciden en su equipamiento y en todos aquellos elementos que condicionan la efectividad de la misma. El "planeamiento por capacidades" ha de evaluar las alternativas posibles para cubrir la carencia de cada capacidad militar, debiendo considerarse, a la hora de concretar los sistemas y su soporte logístico, la disponibilidad de la tecnología adecuada para poder alcanzar la capacidad requerida en el escenario correspondiente.

Se ha denominado "revolución logística" el conjunto de drásticos cambios a introducir en los procesos de obtención que se desarrollaban, para adecuarlos a las exigencias que los procesos de transformación acarrean. Éstos requieren más agilidad, más flexibilidad, mayor control del coste de ciclo de vida, menor riesgo, plazos de tiempo mucho más cortos y ajustados y, sobre todo, una mayor garantía de elección de la tecnología adecuada. Si quisiéramos sintetizar, los componentes primordiales de esta revolución logística son la búsqueda de la superioridad tecnológica especialmente en la gestión de la información, y el cambio en las relaciones de las Fuerzas Armadas con la industria.

Se está viendo que el calado de esta revolución logística es muy superior al inicialmente supuesto y que está arrastrando a organismos gubernamentales e industrias a una nueva forma de percibir "el negocio de defensa". Por ejemplo en

Estados Unidos el Departamento de Defensa ha generado recientemente (junio, 2006) un Documento *Business Transformation Guidance* que introduce las pautas para la "transformación del negocio" de cara a alinear la forma de gestionar con la obtención de las capacidades militares. En este Documento se refleja claramente la importancia de la gestión de la información y la estrategia orientada al entorno de red global.

En este apartado de esta *Monografía*, considerando necesario no repetir contenido con los apartados anteriores y el elevado nivel de innovación del entorno, que hace que lo publicado antes del año 2004 sea historia, vamos a centrarnos en:

- Un análisis del tratamiento de la gestión tecnológica en el marco de los procesos de obtención actuales de las Fuerzas Armadas de algunos países de nuestro entorno, y el enfoque de la gestión tecnológica de la información en las organizaciones.

- Un análisis de la evolución promovida por la transformación de las Fuerzas Armadas en la gestión de la información: el concepto NNEC (*NATO Network Enable Capability*) y la revitalización de la ingeniería,

- Un análisis de los elementos que integran la gestión tecnológica hoy en día, resultante de haber estudiado en profundidad tanto las prácticas actuales de los responsables de las adquisiciones, como las de los responsables operativos.

- Un análisis de las iniciativas emergentes en los paises avanzados, que marcan "la tendencia" en gestión tecnológica y que previsiblemente constituirán la forma habitual de enfocar la innovación tecnológica en los próximos años.

- Una brevísima síntesis de la forma actual de abordar la gestión tecnológica de las Fuerzas Armadas en España que ya se describe en otro capítulo de esta *Monografía.*

- Y finalmente un esbozo de los retos para embarcarse en la adopción de la "tendencia" citada.

La gestión tecnológica en el marco de los procesos de adquisición desarrollados por las Fuerzas Armadas de los países avanzados

Las Fuerzas Armadas son conscientes de que los retos a los que tendrán que enfrentarse en el siglo XXI sólo serán superables gracias a la innovación tecnológica. De su capacidad de realizar una gestión tecnológica “adecuada” dependerá que puedan disponer de medios que resulten efectivos para las misiones que deban realizar en los futuros escenarios ante las amenazas previsibles e imprevisibles. Igualmente, el que puedan conseguir una reducción significativa de los tiempos de obtención, la implantación de una nueva logística más eficaz, el que se disminuya el riesgo de obsolescencia prematura del equipamiento y el que se optimice el coste total de propiedad de cada sistema dependerá, en gran parte, de que se realice una gestión tecnológica adecuada.

Pero ¿qué significa gestión tecnológica adecuada? Evidentemente no es lo mismo para todas las Fuerzas Armadas, ya que dependerá en cada caso de su tamaño, su presupuesto, su nivel de participación en conflictos y misiones de paz, etc, etc. Además la gestión tecnológica debe ser flexible y dinámica, adaptándose continuamente a las demandas de los nuevos escenarios operativos y promoviendo la generación de nuevas potencialidades y sinergias en la base industrial. Por ejemplo en Estados Unidos, dado el carácter singular de la lucha contra el terrorismo, que demanda una generación de tecnología mucho más rápida, una base industrial mucho más amplia y abierta a pequeñas empresas emprendedoras, y una forma de contratación mucho más dinámica e interactiva gobierno-empresas, han creado la “superagencia” TSWG. Esta organización es la responsable de la contratación de programas de innovación tecnológica para más de 80 grandes organismos de una forma centralizada y con unos nuevos procesos de contratación.

A nivel de la Unión Europea las naciones están apostando por la Agencia Europea de Defensa (EDA) como herramienta potencial de integración tanto de tecnologías como de adquisiciones. Lo que es común, es que hoy en día todas las naciones están implantando unas políticas conducentes a la identificación, priorización, evaluación y protección de las tecnologías de su interés. Y estas políticas forman parte de unas políticas más generales: las políticas de adquisiciones.

A continuación se incluyen, para naciones y organismos de referencia, una serie de consideraciones sobre cómo es el marco en la gestión de adquisiciones y los aspectos industriales y tecnológicos, y cómo es su gestión tecnológica en general y

su política tecnológica para los sistemas de información y la evolución a NNEC en particular. No se ha considerado pertinente uniformizar el contenido (por ejemplo comparando organizaciones, políticas y directivas) en cuanto que el contexto es diferente en cada caso. Lo que importa aquí es mostrar el cambio experimentado por la gestión tecnológica en los últimos tiempos como consecuencia de los procesos de transformación y como se explicita la relación de tecnologías de interés prioritario para las Fuerza Armadas.

Estados Unidos

En Estados Unidos las bases para la actividades de defensa incluyen los siguientes Documentos QDR (*the Quadrennial Defense Review*), NDS (*the Nacional Defense Strategy*) y NMS (*the Nacional Militar Strategy*). En ellos se establecen una serie de objetivos de defensa para las actuaciones del Departamento de Defensa (DoD).

Uno de estos objetivos del DoD es que el combatiente disponga de tecnología superior y a la vez financiable, que apoye la realización de sus misiones y le proporcione capacidades revolucionarias.

El Programa del DoD de Ciencia y Tecnología (S&T) está coordinado y se focaliza a través de cinco Documentos: *the Defense S&T Strategy*, *the Defense Technology Area Plan*, *the Defense Technology Objectives document*, *the Joint Warfighting S&T Plan* y *the Basic Research Plan*. Estos Documentos se complementan con S&T master plans de los diferentes ejércitos y agencias.

The Defense S&T Strategy establece áreas de inversión de alta prioridad y designa a un ejército o a una agencia como lider de la investigación de cada área con unos objetivos determinados. Este proceso se llama *Reliance*. Incluye los esfuerzos en investigación desarrollados por los tres ejércitos, *the Ballistic Missile Defense Organization*, *the Defense Threat Reduction Agency*, *the Defense Advanced Research Projects Agency*, *the Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts* y *the Joint Staff*.

The Defense Technology Area Plan documenta los esfuerzos planificados del DoD en ciencia y tecnología exponiendo el fin, el contenido y los principales objetivos del esfuerzo. El Plan define la estrategia de investigación aplicada y tecnología

avanzada de las 12 tecnologías claves. Adicionalmente se documenta *the Defense Technology Objectives* con los objetivos tecnológicos (aproximadamente 200) que conforman el Programa de S&T.

Con la correlación de estos Documentos el DoD asigna específicamente objetivos ligados a las tecnologías clave y logros esperados a cada ejército o agencia.

JWSTP (*The Joint Warfighting S&T Plan*) es semejante a *the Defense Technology Area Plan* salvo que los esfuerzos que documenta son conjuntos. Su relevancia creciente radica en que es la base para la evolución de las capacidades conjuntas y por tanto va ganando protagonismo con el proceso de transformación.

The Basic Research Plan es el Documento que presenta los objetivos del DoD para los Programas de Investigación Básica que mayoritariamente realizan las universidades con financiación del DoD.

Respecto a la gestión de adquisiciones, los documentos clave del DoD son: la directiva 5000.1 la instrucción 5000.2 y la guía DAG (*Defense Acquisition Guidance*). Dentro de estos Documentos se contempla la adquisición de tecnología. Concretamente en el capítulo 7 de la DAG se exponen las indicaciones para adquirir tecnología de la información y sistemas de seguridad nacionales y muestra que el Departamento de Defensa ha de cumplir una serie de requerimientos formales para adquirir Sistemas IT y NSS y está utilizando una estrategia network-centric para transformar las capacidades militares, de negocio y de inteligencia.

El 7 de Junio de 2005 se publicó, por el *Acting Deputy Secretary of Defense*, la autorización para llevar a cabo una evaluación integrada del proceso de adquisición en el ámbito del DoD. La evaluación debía de cubrir todos los aspectos del proceso, incluyendo requerimientos, organización, aspectos legales, metodología de decisión, controles, comprobaciones, etc. El resultado esperado era recomendar una estructura y unos procesos para desarrollar las adquisiciones en el entorno del DoD con alineamiento de la responsabilidad, la autoridad, y la contabilidad.

Durante el segundo semestre del año 2005 se realizó esta evaluación por un panel nombrado para ello y de acuerdo con el roadmap preparado al respecto. En Enero de 2006 se publicó el DAPA (*Defense Acquisition Performance Assessment Report*).

La visión integrada del estado de las adquisiciones cubrió 42 áreas. Los mayores problemas detectados eran referentes a la vigilancia y liderazgo del proceso. Se constató ineficiencia en las revisiones y problemas de coordinación y entendimiento.

Se consideraron los siguientes elementos: organización, personal, presupuesto, proceso de definición de requisitos, gestión del proceso de pruebas operacionales, proceso de adquisición, cumplimiento de plazos e industria.

Por cada uno de los elementos se explicitó: evaluación del cumplimiento, mayores hallazgos, posibles mejoras del cumplimiento identificadas, y criterios para su implantación

Los resultados de este estudio ya se están notando en las directrices y enfoques generados en estos últimos meses, siendo previsible que alcance un importante impacto en el proceso de adquisición. Los aspectos referentes a la gestión de tecnologías, si bien no han merecido un tratamiento diferenciado en el DAPA, están incluidos en el cumplimiento de plazos (por madurez de las tecnologías), pruebas, industria y otros elementos.

En el Documento *Policy for Systems Engineering* de 20 febrero del año 2004 se establece la necesidad de aplicar, en todas las adquisiciones, una disciplina rigurosa de ingeniería de sistemas. Se considera muy importante, para que el DoD tenga la posibilidad de afrontar el reto de desarrollar y mantener la capacidad militar que necesita para las operaciones. El enfoque futuro debe centrarse pues en ingeniería y en tecnología.

Par el DoD, la gestión técnica y la gestión tecnológica son inseparables en la gestión de la información. La inserción de tecnología es un proceso cuyos riesgos deben ser cuidadosamente analizados La orientación a servicios y el tratamiento de los datos son igualmente claves. Se reconoce la necesidad de una revitalización de la ingeniería.

El contexto pasa de ser el sistema a ser la familia de sistemas, el Sistema de sistemas y la NCW (*Net-Centric Warfare*). El concepto sistema de sistemas ligado a la transformación marca un antes y un después en la forma de diseñar y construir sistemas. Los sensores, plataformas y armamentos pierden el tratamiento de

“adquisiciones independientes”. La GIG (*Global Information Grid*) es el elemento posibilitador a estudiar. Tan importante es definir el escenario futuro como establecer un camino viable para llegar a él. Cobra pues importancia el concepto de *roadmap*.

Pero si el proceso de transformación ha tenido implicaciones para algún tipo de sistemas, ha sido sin lugar a dudas para los Sistemas de Información. No sólo han evolucionado su naturaleza sino su enfoque (a servicios), su forma de desarrollo (evolutivo), su tecnología, la exigencia de interoperabilidad, el tratamiento de los sistemas legacy, la seguridad, la financiación, la validación y aceptación, etc.

Con respecto a los procesos de transformación el DoD ha publicado muchos documentos que dejan claros los objetivos y las pautas a seguir. Son ejemplos: *the Transformation Planning Guidance*, *the Army Transformation* y *the Transformation Trends* y los diversos roadmaps sobre transformación a nivel de cada Ejército. En todos estos documentos es un invariante la evolución a la NCW como factor posibilitador de la transformación.

El término NCW describe la combinación de tácticas emergentes, técnicas y procedimientos que una fuerza conectada total o parcialmente a través de una red puede emplear para disponer así de una ventaja en la lucha. Lo importante es la acción: “conectarse” más que el medio: “la red de conexión”. NCW, según la Oficina de Transformación de la Fuerza, es una teoría de la guerra emergente porque identifica nuevas fuentes de poder (compartición de información, acceso a la información, velocidad), cómo estas fuentes se relacionan, cómo se busca la consecución de objetivos y su relación con los objetivos nacionales. Así descrito más parece una filosofía que un enfoque pragmático, pero en el año 2004 se utilizó ya la *Net-Centric Checklist* durante la revisión de los programas del DoD de tecnología más compleja para asegurarse de la inclusión de capacidades net-centric en las plataformas. En la lista del DoD de programas militares clave hay una serie de ellos relativos a NCW. Entre estos se encuentran los Programas: *Net Centricity*, DoD GIG, AT3 (*Air Force Advanced Tactical Targeting Technology*), *Air Force Link 16*, CEC (*Navy Cooperative Engagement Capability*), FBCB2 (*Air Force XXI Battle Command Brigade and Below*), JTRS (*Joint Tactical Radio System*) y J-UCAS (*Joint Unmanned Combat Air Systems*).

La evolución a NCW está ya madura para el DoD. Ha quedado explicada en documentos formales de justificación (por ejemplo el *report* al Congreso *Network Centric Warfare: Background and Oversight Issues for Congress* 18 de marzo de 2005), en documentos de tipo técnico (por ejemplo *the Guide for Implementing Net Centric Data Sharing* o *the DoDAF* (marco de arquitectura del DoD)), en documentos de procedimientos (por ejemplo DIACAP (*Defense Information Assurance Certification and Acreditation Process*) y sobre validación de servicios proporcionados por *the GIG*) y en los múltiples foros industriales.

Reino Unido

En el Reino Unido el *White Paper* del Ministerio de Defensa (MoD) de 2004 marcó la política del gobierno en materia de defensa.

En el proceso de planeamiento de capacidades, el documento *the Defence Strategic Guidance* es el que presenta los futuros requerimientos de capacidades militares con un horizonte de 15 años. También dentro de este proceso, el documento *the Defence Planning Assumptions* establece a cinco años lo que deberían ser capaces de hacer las fuerzas armadas y los parámetros referentes a la estructura de la fuerza, y el documento *the Future Capability Development* marca para los responsables los requerimientos de las capacidades militares a obtener.

Respecto a la gestión de adquisiciones, desde hace años se sigue y se perfecciona en el ámbito del MoD el proceso de adquisiciones denominado *Smart Acquisition*.

El AMS (*Acquisition Management System*) es el conjunto de directrices, políticas, y mejores prácticas y procedimientos relativos a las adquisiciones de sistemas realizadas bajo *Smart Acquisition*. Este sistema es evolutivo y se ha podido comprobar a través de los años cómo han ido incorporándose aspectos emergentes como los procedimientos relacionados con el planeamiento de capacidades y con NNEC.

La intranet del MoD pone a disposición de los expertos el material sensible que no se difunde con acceso publico, facilitando el trabajo y la interrelación entre los expertos y entre organizaciones. Se han creado intranets específicas para comunidades de interés: por ejemplo CABINET es la *CApability Based InterNET*.

Un brevísimo resumen de la organización y sus funciones según la *Smart Acquisition* es el siguiente:

- Los participantes en el ciclo de vida de los sistemas por parte del MoD son la DPA (*Defence Procurement Agency*) y la DLO (*Defence Logistic Organization*) junto con el ECC (*Equipment Capability Customer*) y el segunda *Customer* MoD.

- La DPA es la agencia responsable de la adquisición de los sistemas que se determinan mediante el planeamiento de capacidades que realiza en el ECC.

- La DLO es la agencia responsable del apoyo logístico de los sistemas interaccionando con el usuario (segunda customer).

- El CADMID (*Concept, Assessment, Demonstration, Manufacture, in Service, Disposal*) es el modelo de ciclo de vida (ciclo de adquisición) dentro del ámbito del MoD. Existe un proceso definido de "generación" de casos para la adquisición de capacidades con puntos de aprobación definidos antes y después de la fase de Assessment.

- El MoD lleva a cabo una gestión completa del ciclo de vida de la obtención de capacidades: TLCM (*Through life capability management*).

En la gestión de capacidades se tienen en cuenta las DLOD (*Defence Lines of Development*): entrenamiento, equipamiento, personal, información, conceptos y doctrina, organización, infraestructura y logística. Son el equivalente al MIRADO nacional de la división de Estrategia y Planes del EMACON.

Los *Capability Working Groups* son grupos que proporcionan soporte a los responsables de las distintas capacidades (pertenecientes al ECC).

Los *Integrated Project Team* (Oficinas de Programa) son los grupos multidisciplinares de composición variable que se crean y trabajan como responsables durante todo el ciclo de vida de los sistemas. Pertenecen a la DPA.

Forma también parte de las iniciativas que cubre la *Smart Acquisition* una interrelación nueva y más intensa con la industria.

Cada agencia define anualmente sus planes comunicando sus objetivos e indicadores para medir su cumplimiento y los correspondientes roadmaps. Por ejemplo la DLO publica el *Balanced Scorecard* lo que permite evaluar los resultados de su gestión.

Con respecto a los aspectos tecnológicos e industriales en el seno del MoD los documentos que se consideran fundamentales son *Defence Industrial Strategy* conocido como DIS (*Defence White Paper*) publicado en diciembre de 2005, EAC (*Enabling Acquisition Change)* publicado en junio de 2006 y el reciente DTS (*Defence Technology Strategy for the demands of the 21st century*) (publicado el 15 de octubre de 2006.

El Documento DIS es sin duda el elemento más importante para marcar la política de adquisiciones e industrial de los próximos años para el Reino Unido. Es consecuencia de una reflexión realizada en el seno del MoD sobre la gestión de capacidades y la demanda industrial. Se ha llegado a la conclusión de que salvo Estados Unidos ningún país puede permitirse apostar al desarrollo tecnológico de todas las tecnologías y por lo tanto es necesario realizar una priorización que indique a la industria las áreas tecnológicas en las que focalizarse. La priorización debe reflejar las capacidades industriales que se considera necesario retener en el Reino Unido.

El Documento DIS consta de tres partes: una primera parte donde se expone el contexto estratégico, una segunda parte donde se revisan las perspectivas por sector industrial y tecnologías transversales y una tercera parte donde se indican los retos para el cambio.

En la primera parte se analiza el reenfoque que va a precisar hacer la industria, para evolucionar de una industria que ha estado en los últimos años fabricando grandes plataformas a una industria que mayoritariamente se centrará en modernizaciones y upgradings. Igualmente se examinan las exigencias de innovación tecnológica y su materialización. Por ejemplo un reto a afrontar va a ser cómo posibilitar la inserción rápida de tecnología ante nuevas amenazas. Asimismo incluye un apartado sobre como identificar y sostener las capacidades industriales clave.

En la segunda parte del Documento son objeto de análisis los siguientes sectores: ingeniería de sistemas, sector naval, vehículos blindados, plataformas de ala fija, helicópteros, munición, armas complejas, C4ISTAR, protección química, biológica, radiológica y nuclear, tecnologías prioritarias para facilitar las capacidades de defensa, pruebas y evaluación.

En la tercera parte se indican los retos clave: planear mejor, invertir en ingeniería de sistemas, mayor interrelación con la industria, mayor difusión y comunicación, apuesta por sistemas abiertos y trabajo conjunto con énfasis en el desarrollo y la formación del personal.

El Documento EAC (*Enabling Acquisition Change*), también denominado informe MacKane, representa la reflexión, tras la publicación de la DIS, de cómo afrontar la puesta en marcha de esta estrategia industrial en los próximos años. A parte de establecer un marco a largo plazo, la DIS mostraba la necesidad de modificar el proceso de enfocar al adquisición de capacidades. Como respuesta, en el documento EAC se ha consolidado el concepto TLCM (*Through Life Capability Management*), como el nuevo enfoque mediante el que ha de plantearse la obtención la adquisición y el servicio de una capacidad desde el principio al fin.

El EAC ha sido generado por un pequeño equipo muy cualificado y con visión de futuro que propone cambios en la forma de actuar el MoD en los procesos de adquisición. Se espera que tengan una repercusión significativa a largo plazo.

Las propuestas básicas de este informe son:

- Mejorar la planificación financiera del MoD para asegurarse de que en las decisiones que se tomen se consideran mejor los costes totales de los sistemas (*Whole Costs*) o concepto equivalente TOC del DoD) teniendo una visión estratégica presupuestaria de los próximos diez años.

- Fomentar los procesos incrementales de adquisición y la implantación del citado TLCM.

- Plantear la fusión de las dos agencias: la DPA y la DLO para el 1 de abril de 2007.

El Documento DTS, publicado en octubre de 2006, muestra por primera vez el enfoque de la Investigación y el Desarrollo (I+D) (R&D) que se había prometido en la DIS en diciembre de 2005. Presenta de forma integrada, en un auténtico ejercicio de gestión tecnológica, el esfuerzo del MoD, de otras organizaciones gubernamentales, de la industria y de la universidad.

Consta de tres partes: una introducción donde describe el contexto estratégico y el enfoque, una segunda parte integrada por un análisis de cada sector y de las tecnologías transversales y una tercera parte que muestra como implementar la DTS. Se incluyen adicionalmente, como anexos, una tabla resumen de priorización de las tecnologías y la innovación en la cadena de suministro que representan los árboles de tecnología construidos al respecto.

En suma, a través de la DTS, el Ministerio de Defensa del Reino Unido explicita: sus prioridades para I+D, la forma de financiación, las competencias y conocimientos que serán imprescindibles, la necesaria mejora de sus procesos, y las posibles oportunidades y áreas de colaboración en investigación a nivel internacional.

Dada la novedad de este Documento, junto con que muchos de los problemas y planteamientos que hace son extrapolables a nuestro contexto, se ha considerado adecuado extenderse en su exposición con una breve síntesis de la situación de partida y de la estrategia propuesta.

Los puntos críticos detectados, al llevar a cabo una revisión de la estrategia tecnológica del MoD, fueron:

- La amenaza actual convierte en fundamental para la capacidad militar la ciencia y la tecnología.
- Hay necesidad de combinar más la inversión que realizan el gobierno y la industria en I+D.
- Actualmente se focaliza el esfuerzo en madurar las tecnologías actuales en detrimento de las tecnologías emergentes.
- La inversión en I+D de la industria es baja respeto a la inversión del MoD.

- Son esenciales tanto competencias y habilidades en investigación de primera clase como “expertise” en tecnología y ciencia.

- El MoD debe poseer y controlar tecnologías clave. Por ejemplo la arquitectura del sistema de Sistemas C4ISTAR.

La información clave incluida en el Documento DTS comprende:

- Las áreas prioritarias de ciencia y tecnología en las que desarrollar I+D.

- Las áreas críticas para la seguridad y soberanía de la nación.

- Las oportunidades claras de colaboración con la industria, universidades y países aliados.

- Cómo adaptar e integrar componentes y subsistemas de procedencia exterior.

- Dónde mantener “expertise” como cliente inteligente para desarrollar una estrategia adecuada en la adquisición de COTS.

- Nuevas iniciativas par estimular la innovación en la investigación de defensa.

- Las acciones que deben tomar el MoD y la industria para proseguir y explotar los resultados del programa de inversiones de defensa en I+D en cuanto a tecnologías se refiere.

- Como continuar apoyando la base de competencia en ciencia e ingeniería para que sustente tanto al MoD como a la industria.

Dada la continua evolución del entorno, el documento DTS se considera un documento vivo estando prevista su actualización cada aproximadamente dos años.

Como enfoque para acometer la puesta en marcha de esta estrategia en el documento se exponen:

- *Los retos.* El MoD ha de trabajar en colaboración con la industria, la universidad y con posibles *partners*. Hay cuatro componentes a considerar en la puesta en marcha de esta estrategia:

1. Prioridades en ciencia y tecnología.
2. Proceso para agilizar la explotación de resultados.
3. Marco de inversiones MoD/industria.
4. Trabajo con DSTL (organismo de defensa de R&D) y con las universidades.

- *Las prioridades en ciencia y tecnología.* Se explicitan las prioridades para los distintos sectores. En particular para NNEC se dice: “NNEC es fundamental para el éxito de la misión y debemos ser más efectivos que nuestros adversarios usando y controlando la información”. En consecuencia el MoD reconoce esencial ostentar el rol de propietario y el liderazgo en el establecimiento de una “comunidad de práctica” para diseñar y desarrollar la arquitectura del Sistema de sistemas C4ISTAR.”

- *El proceso para agilizar la explotación de los resultados de la I+D (R&D).* Basándose en las técnicas del AMS para medir y controlar la evolución en madurez de las tecnologías se enfocan medidas para agilizar la inserción.

- *El marco de inversiones MoD/industria.* El enfoque de este punto hasta ahora ha sido suponer que sobre la primera parte del ciclo de vida de una tecnología, esto es hasta que alcanza un cierto nivel de madurez la inversión la realizaba el MoD y a partir de este punto hasta alcanzar su madurez la industria. Esto habrá de replantearse en el futuro caso a caso, ya que la DTS plantea la colaboración en el tiempo (lo que conlleva dificultades para materializarse).

- *El trabajo con DSTL y con las universidades.* El DSTl, como centro/laboratorio propio de I+D, es la mayor fuente de “expertise” científica y tecnológica del MoD. Se considera vital que el Dstl mantenga estas capacidades necesarias para cumplir su función. Esto se hará mediante la investigación interna y trabajando con la industria.

- *Una cadena de suministro que estimule y explote la innovación.* La innovación del equipamiento militar contribuye a proporcionar una ventaja estratégica al dar una ventaja tecnológica sobre el oponente. Para estimular la innovación el MoD ha

tomado como referencia a la agencia de Estados Unidos DARPA que plantea y busca resolver los retos tecnológicos a afrontar. El MoD querría disponer de la capacidad o habilidad de DARPA para estimular la generación de ideas innovadoras y llevar a explotación aquellas que parecen ser más prometedoras.

Por otra parte el MoD ha conseguido que la industria, gracias al DIC (R&T) *Sub-group*, genere unos árboles de tecnologías. Estos se incluyen en el anexo B de la DTS, representando una novedad significativa en cuanto que se configuran nichos por tecnología en vez de por productos. Es también interesante en este anexo la consideración de la naturaleza y contribución en la innovación del equipamiento de las fuerzas armadas de los posibles distintos *partners*: grandes empresas, pequeñas empresas y Pymes, centros de investigación, y universidades.

Otros documentos importantes recientes son:

- El DPA/DLO publicado en Julio de 2006. Este documento presenta los cinco principios clave para la gestión tecnológica. Estos cinco principios, en resumen, son analizar las oportunidades tecnológicas, gestionar los riesgos tecnológicos, planificar conjuntamente los recursos, entrenar adecuadamente al personal y trabajar conjuntamente con la industria.

- El ECC de junio de 2006.Este documento presenta cómo identificar los objetivos de capacidad, cómo identificar las Medidas de Efectividad (MOE,s), y como realizar un benchmarking para cuantificar el objetivo de capacidad usando las MOE,s.

El Ministerio de Defensa del Reino Unido ha difundido el concepto NNEC mediante el Documento *Joint Service Publication 777-Network Enabled Capability* que recoge los objetivos y el enfoque para la implantación de NNEC y busca promover la creatividad y el debate para orientar y facilitar su futuro desarrollo.

Alemania

En Alemania la publicación de las directrices de política de Defensa en mayo de 2003 inició la reorientación de las Fuerzas Armadas. Los cinco documentos formales relevantes para el futuro son: *Directive on the Development of the Bundeswehr* (1 de octubre de 2003), *Directive on the Development of the Armed Forces* (1 de marzo de

2004). *Concept for the Bundeswehr* (9 de agosto de 2004), *Directive on the Development of the Army* (5 de julio de 2004), y *The Army in Transformation* (1 de diciembre de 2004). Junto a estos la reorganización del mando del Bundeswehr ordenada el 21 de enero de 2005 marca las nuevas directrices de las fuerza alemanas.

Con respecto a los cambios en la gestión de adquisiciones hay que destacar una apuesta firme por la EDA, cuyo enfoque tecnológico expondremos más adelante. Asimismo es importante destacar el cambio significativo en las relaciones entre el Bundeswehr y la industria, para lo cual en 1999 se firmo un acuerdo estratégico de partenariado. Para su implementación se estableció el *Gesellschaft für Entwicklung, Beschaffung und Betrieb* propiedad del Gobierno alemán y a su vez copropietario de las industrias. Esto significa que Alemania apoya que su industria mantenga una clara identidad a nivel europeo, aunque colabore en la puesta en marcha de la EDA como una institución capaz de crear y poner en marcha un nuevo modelo de cooperación en defensa en la Unión Europea.

Francia

Las orientaciones estratégicas actuales provienen mayoritariamente del *Libro Blanco de la Defensa de 1994*. La Ley de Programación Militar (LPM) 1997-2002 introdujo un modelo de ejércitos para el 2015. La LPM 2003-2008 ha confirmado estas orientaciones con la introducción de las lecciones aprendidas en las crisis y conflictos recientes y la consideración de la amenaza terrorista global.

Actualmente Francia elabora cada año el Documento *Le Plan Prospectif a 30 Ans* que muestra la preparación para afrontar el futuro, orientando los estudios y la investigación. Existe un modelo de fuerzas armadas para el 2015 que ha sido establecido por los Estados Mayores, y un modelo de capacidades tecnológicas que Francia ha generado identificando las tecnologías a adquirir.

El Documento citado muestra lo significativa que se considera la innovación tecnológica y establece la estrategia en materia de obtención del equipamiento de las fuerzas. Igualmente aparecen claramente definidos los objetivos tecnológicos en forma de tecnologías

El Plan consta de un primer punto sobre “como preparar el futuro” utilizando un análisis de prospectiva basado en un ejercicio de integración de la prospectiva operacional, la prospectiva geoestratégica y la prospectiva tecnológica. En el segundo punto describe la evolución previsible e imprevisible y el auge de las tecnologías de la información. En el tercer punto expone la estrategia militar general, explicitando las consideraciones generadas sobre la disuasión, la prevención, la protección y la proyección. En el cuarto punto contempla la prospectiva operacional con la tipología de las confrontaciones futuras.

En el quinto punto se exponen los trabajos de prospectiva tecnológica, que por ser el objeto de este libro vamos a describir con más detalle que el realizado con los otros puntos. Los trabajos se integran en dos grupos: la oferta tecnológica que es el resultado del esfuerzo de evaluar por anticipado las tecnologías por una red integrada por la DGA y organizaciones exteriores (ONERA, CEA, CNRS, universidades, etc.) y los estudios tecnológico-operacionales que relacionan las necesidades y la definición de conceptos técnicos susceptibles de satisfacerlas.

El horizonte 2030 es el que se considera para realizar la prospectiva tecnológica. Las tendencias más importantes identificadas para ese horizonte incluyen:

- La miniaturización de sistemas.
- La concepción y desarrollo de metasistemas o sistemas de sistemas.
- La puesta en red de objetos y sistemas.
- La electrificación de los sistemas y la evolución de la gestión de energía eléctrica.
- La utilización generalizada de la tecnología digital.
- La integración del hombre con los sistemas de armas.
- La robotización de los sistemas.
- La mejora de la capacidad de .reacción de los sistemas.
- Los recursos espaciales.

- La toma en consideración de las limitaciones jurídicas.

Entre los dominios tecnológicos serán de interés significativo las biotecnologías y las nanotecnologías. Asimismo será importante el enfoque multidisciplinar, la renovación rápida de las tecnologías y la utilización cruzada con el ámbito civil.

En el sexto punto se presenta la prospectiva de los sistemas de fuerzas. La prospectiva de los sistemas de fuerzas se apoya en dos tipos de herramientas complementarias e interactivas: los proyectos federados y las capacidades tecnológicas. Un proyecto federado es un proyecto que reagrupa en un conjunto ordenado y coherente los trabajos para preparar según el plan tecnológico, los futuros programas de armamento y/o para mejorar una capacidad operacional dada cuantificada por objetivos explícitos.

En este punto se muestran como temas “transversales” dos temas: el espacio y las operaciones centradas en red (les opérations réseaux-centrées). Para este último tema se constata el avance en los últimos años, la dinámica de cambio y su relevancia. También se analizan los principios de las operaciones centradas en red y se exponen una serie de recomendaciones para las tecnologías de la información.

Asimismo dentro del punto sexto se analizan la prospectiva específica de los siguientes sistemas de fuerza:

- Sistemas de disuasión.
- Sistemas de mando, conducción, comunicaciones y reconocimiento.
- Sistemas de proyección y movilidad.
- Sistemas submarinos.
- Sistemas para el dominio del medio aeroterrestre.
- Sistemas para el dominio del medio aereomarítimo
- Sistemas para el dominio del medio aeroespacial.
- Sistemas para la preparación y el mantenimiento de la capacidad operacional.

Con respecto a la política tecnológica de Francia es igualmente importante destacar el decidido impulso a los partenariados con la industria y su apuesta firme por la EDA.

No obstante un aspecto que algunos consideramos se percibe en las actuaciones de los responsables franceses, es el interés en llegar a acuerdos bilaterales con otros países, en aquellos desarrollos tecnológicos en los que las empresas francesas pueden alcanzar un posicionamiento dominante, mayor que el que obtendrían si el desarrollo tecnológico se realizase a nivel de organismo multinacional.

La EDA

La EDA (*European Defence Agency*) es sin duda uno de los ejemplos más claros de enfoque de futuro en la gestión tecnológica. Por ello vamos a analizarla con más detalle. Tanto su estructura, que contiene una Direccion de Investigación y Tecnología, entre las cuatro Direcciones existentes, como la estrategia que se ha definido, dan lugar a un amplio campo de actuación de fomento del desarrollo tecnológico de los países de la Unión Europea.

La denominada *Joint action 2004/551/CFSP* establece que la Agencia deberá promover la efectividad de la investigación y tecnología de la defensa europea, y define las principales funciones y tareas de la agencia en este campo para lograr su objetivo. El reto es sin duda lograr la colaboración entre los países. Dado que sólo el 1,31% del gasto total europeo en defensa se dedicará en 2006 a Investigación y Tecnología (I+T) y que sólo el 14,2% se invertirá en colaboraciones entre países miembros (fuente EDA) esta claro por qué la Agencia considera que tiene un gran territorio potencial por cubrir.

Para hablar de la contribución de la EDA vamos a centrarnos en tres puntos: la organización para I+T (y los *Captechs* en particular), el Documento clave de enfoque *An Initial Long Term Vision for European Defence Capability and Capacity Needs* y la celebración de la Conferencia sobre I+T (R+T) en febrero 2006 como revisión de la situación y declaración pública de que el I+T es fundamental de cara al futuro.

El 22 de abril de 2005 el *Steering Board* decidió la aprobación de las reglas del concepto operacional del I+T:

1. *Orientación a capacidades:*

   - Segmentación del campo tecnológico en tres bloques correspondientes a tres dominios de capacidad: IAP (*Information Acquisition & Processing Knowledge*), GEM (*Guidance, Energy & Materials*) y ESM (*Environment, Systems & Modelling*). El primer dominio corresponde a áreas de capacidad de "conocimiento"(informar y mando), el segundo a *engagement* (participar y proteger) y el tercero a "maniobra" (proyectar, sostener).

   - Correlación de estos tres bloque con áreas de tecnología denominadas Captechs, de forma que se definen 12 *captechs*, cuatro por cada uno de los bloques citados: componentes, sensores, proceso de señal y CIS y redes de comunicaciones para el primer bloque, materiales, sistemas de energía y propulsión, protección y letalidad y control y guiado para el segundo bloque y diseño, simulación, entorno operacional y factores humanos para el tercer bloque.

   - Emisión de criterios para evaluación de la contribución de los proyectos a las capacidades.

2. *Gestión centralizada.*

   - Establecimiento para cada *Captech* de una red de expertos incluyendo representantes de la industria y de centros de investigación, con personal propio de la EDA como promotor de actuaciones y de contactos entre *captechs*.

   - Control del progreso de los trabajos y organización de *workshops* y seminarios.

3. *Transparencia a través de monitorización e informes:*

   - Generación y mantenimiento actualizado de un *roadmap* propuesto por la Agencia y basado en la visión a medio-largo plazo.

   - Consulta entre reuniones con responsables nacionales. Coordinación con directores de Armamento.

   - Medición mediante indicadores del resultado de la cooperación e informe a usuarios finales.

4. *Acuerdos de transferencia con redes de cooperación existentes:*

   - Invitación a grupos de trabajo y redes existentes para traspaso de su actividad a la EDA bajo las formas de actuación de ésta.

5. *Interfaz con la investigación civil y de doble uso:*

   - Identificación de potenciales sinergias por los *captechs* buscando la no duplicación en áreas de potencial uso dual.

   - Asesoramiento en prioridades para la investigación en seguridad.

6. *Relación con la industria:*

   - Participación de la industria en los *captechs*.

   - Reconocimiento de ideas y propuestas de la industria.

   - Directrices para aprobación de proyectos de la industria en función de las carencias de capacidades detectadas.

   - Identificación in situ de capacidades industriales y capacidades técnicas y centros de excelencia por los distintos *captechs*.

7. *Utilización de la EDA como organismo contratante de I+T:*

   - Dotación de fondos para estudios de I+T ligados a prioridades orientadas a capacidades.

   - Soporte de la Agencia a contratación de proyectos de cooperación.

En consecuencia, la aplicación de estas reglas conducirá a:

- La organización de la Dirección de I+T en la EDA.

- La interrelación con las otras tres direcciones.

- Visibilidad desde el nivel de toma de decisión de la estrategia y los resultados en el marco de la EDA.

- Capacidad de identificar prioridades basadas en carencias de capacidades.
- Participación de la industria en el proceso activa y controlada.
- Propuestas de acoger las actividades de la WEAG.
- Dialogo con la Comisión Europea sobre investigación de doble uso y en materia de seguridad.
- Capacidad de analizar y proporcionar datos para el estudio de la base industrial.

El Documento *An Inicial Long-Term Vision for European Defence Capability and Capacity Needs* de 3 de octubre de 2006 analiza las perspectivas y las futuras capacidades considerando la necesidad de adaptarse a un cambio en el rol de la fuerza (por una mayor interrelación entre las actuaciones militares y políticas) y una revolución tecnológica.

En el Documento se expone que:

- Las operaciones de seguridad y defensa europeas serán en el futuro expedicionarias, multinacionales y con equipamiento múltiple.
- Las caracteristicas clave de la futura fuerza y su capacidad serán la sinergia, la agilidad, la viabilidad de selección entre un rango de capacidades, y la sostenibilidad.
- Para definir el perfil esperado en las seis áreas de capacidad: mando, información, engage, protección, despliegue y sostenimiento habrá que considerar cuestiones clave: explotación del conocimiento, interoperabilidad, balance de recursos humanos, adquisición rápida, política industrial y flexibilidad ante lo imprevisto.

El Documento no trata de ser un roadmap sino de ofrecer direcciones a seguir, proponiendo una visión de cómo serán las cosas.

Respecto a la gestión tecnológica, el documento identifica a la industria como el máximo generador de tecnología y conocimiento y a la tecnología de la información como el elemento clave de la revolución. Y expone que se deberá ser capaz de

explotar mejor las capacidades civiles y de poder combinar e integrar tecnologías de distintas líneas de desarrollo.

La conferencia sobre investigación y tecnología celebrada el 9 de febrero de 2006 *Research and Technology-an imperative for european defense* sirvió para exponer de nuevo, por parte de la EDA, que la I+T es la llave para la transformación de las fuerza armadas, que los responsables piensan que en Europa se debe gastar en I+T más, mejor y de forma conjunta, que la I+T es fundamental para la salud de la industria y que los Estados Unidos invierten cinco veces más que Europa. Cómo ejemplo se mencionó a la agencia americana DARPA que invierte por encima de tres billones de dólares, lo que es más que todos los países de la Unión Europea juntos. Gastar más en momentos de austeridad presupuestaria no es posible y se habló de redireccionar fondos en una racionalización para evitar duplicaciones de medios e infraestructuras. Gastar mejor puede lograrse invirtiendo en tecnologías clave para el futuro, insertando nuevas tecnologías en plataformas operativas y reduciendo los tiempos de obtención ajustándolos a los del mundo civil.

La conferencia sirvió para definir los cuatro instrumentos, a nivel Unión Europea, necesarios para desarrollar la ”visión” de la EDA. Estos son: un *Defence Science & Technology Board*, una red de expertos en tecnología, una incubadora tecnológica que genere enfoques rompedores y una red de centros de excelencia.

Por parte de los representantes de las fuerzas armadas se constató el interés por tener una estrategia de I+T a nivel de la Unión Europea, sin cerrarse a la utilización de tecnologías de terceros (Estados Unidos) y contemplando la garantía del suministro, Igualmente se mostró la necesidad de las Fuerzas Armadas de que se confiera más agilidad a los procesos de generación y de inserción de tecnología, y que la industria muestre una mayor capacidad de emprender, sin que el *push* de tecnología sea desproporcionado frente a los requerimientos reales del usuario.

La participación de la industria fue sustancial para definir los problemas con los que se enfrenta: los gobiernos deben apoyar con fondos, reorganizándose para interaccionar más y mejor con las empresas, anticipándose en la definición y priorización de necesidades, con nuevos enfoques de contratación que favorezcan el dinamismo de la industria y que hagan más atrayentes y rentables los esfuerzos

en innovación de la tecnología, y aprovechando las oportunidades de las tecnologías duales.

La OTAN

La OTAN como organización es objeto de tratamiento en la prensa diaria. Como planificador, gestor de adquisiciones y responsable logístico en menos frecuente su presencia en los medios pero aún así bastante habitual. Describir las funciones, recursos y procedimientos relativos a la gestión de adquisiciones precisaría mucho espacio, en detrimento de lo que se quiere describir en este libro, por lo que ni siquiera el Programa NSIP va a ser tratado. (En el entorno de la OTAN el Programa NSIP es el que proporciona recursos para las inversiones en infraestructuras y medios (por ejemplo para el conocido cómo “Cuartel de Retamares” en Madrid).

Centrándonos en tecnología las entidades más relevantes de la OTAN son la RTO y la NC3A.

La RTO (*NATO Research and Technology Organization*) es el organismo responsible de la investigación y tecnología en la OTAN. Dado su tamaño y presupuesto cubre una amplia variedad de campos tecnológicos: sensores y electrónica, gestión de la información, tecnología de los sistemas de información. recursos humanos, modelado y simulación, análisis de sistemas y conceptos, integración de sistemas, etc. Por razón de ser concisos no vamos a exponer ni el trabajo en cada campo ni los organismos que integran la estructura: *the Research and Technology Board*, *the Research and Technology Agency*, *the Technicals Panels*, etc.

La NC3A es una Agencia que desarrolla los principales programas de investigación en materia de mando y control, Inteligencia y comunicaciones. Uno de los documentos del máximo interés para estudiar el estado de los sistemas de la OTAN y sus tendencias es el denominado *Rolling Plan* de la NC3A que es un Plan de Trabajos a cinco años donde se explicitan objetivos y recursos. Es un documento interesantísimo, de estudio obligado para el que quiera conocer el rumbo de la OTAN en materia tecnológica. Tampoco por razones de espacio puede ser tratado en esta *Monografía*.

Pero si merece la pena centrarse aquí, por tratarse específicamente de temas relacionados con la gestión de información, en dos iniciativas clave: el análisis de viabilidad NNEC y el *roadmap* NNEC de la OTAN. Estas dos iniciativas y los documentos que las soportan van a resultar, sin duda alguna, fundamentales para apoyar el proceso de transformación de la Alianza.

Los NATO SC´s (*Strategic Commanders*) acordaron en Praga el establecimiento de una serie de *Transformational Goals* y *Transformational Objective Areas*. Una de estas TOA,s es la capacidad NNEC. En junio de 2005 el Comité Militar de la OTAN encargó el desarrollo de un marco estratégico para NNEC NNEC SF (*NNEC Strategic Framework*) como forma de describir las actividades necesarias para el desarrollo de NNEC y servir de apoyo a las tomas de decisiones. El NNEC SF se describió en una serie de documentos: NNEC *Vision and Concept, NNEC roadmap(s)*, NNEC *Business Case(s)*, *Compendium of NNEC related Architectures and Detailed Plan.*

En octubre de 2005 el *Consultation, Command and Control Board* aprobó las recomendaciones del estudio de viabilidad NNEC *Feasisibility Study* (versión 2.0) sobre la necesidad de una estrategia para el desarrollo de futuras capacidades C3 basada en el enfoque de un Planeamiento Basado en Capacidades (CBP) y una estrategia para el desarrollo de una infraestructura NII (*Networking and Information Infrastructure*) de soporte técnico a NNEC.

Para el desarrollo de NNEC se ha definido una estrategia de transformación basada en las directrices del mando de transformación de la OTAN. En el volumen primero del estudio de viabilidad se describen las necesidades operacionales de conexión en red de la OTAN y las implicaciones para el desarrollo de soluciones, y otros temas de nivel reservado. En el volumen segundo se recoge expresamente la recomendación referente al *roadmap* NNEC.

El NATO NNEC *roadmap* se centra en exponer las actividades de gestión e implantación, a realizar a corto plazo, para obtener un progreso significativo en NNEC. No cubre todas las capacidades sino un subconjunto básico para desarrollar ciertos atributos derivados del estudio de viabilidad.

El citado *roadmap* publicado inicialmente en Junio 2006 se focaliza en los siguientes aspectos:

- Identificación de atributos clave de NNEC. Describen lo que el futuro NNEC puede proporcionar a la OTAN y los resultados esperados en términos de mejora de accesibilidad de la información, incorporación de herramientas que faciliten el entendimiento intercultural, el trabajo colaborativo, la formación de grupos la sincronización de efectos, la utilización optimizada de los recursos humanos, etc.

- Acciones de gestión. La mejora no ha de incidir solo en las capacidades operacionales sino en la transformación de la organización. Se proponen la introducción de un portal-*web*, de capacidad de prueba y validación de NNEC, el desarrollo de la formación, realización de conferencias, utilización del modelo CMM, etc.

- Desarrollo de conceptos. La focalización en los aspectos operacionales es fundamental para la transformación de las capacidades operacional. Los conceptos emergentes a lo largo de todo el espectro de actividad funcional (despliegue estratégico, logística, etc.) producen nuevos enfoques para mejorar la interoperabilidad.

- Desarrollo de áreas de servicios. El desarrollo e implantación de servicios e interfaces comunes es crucial para las capacidades de conexión en red a través de fronteras funcionales y de fases de interoperabilidad. Los servicios, tal y como aparece en el estudio de viabilidad NNEC se agrupan en:

  1. Servicios de aplicaciones funcionales.

  2. Servicios de integración de información.

  3. Infraestructura de comunicaciones y servicios.

  4. Servicios de seguridad de la información.

  5. Servicios de gestión de servicios.

- Alineamiento con programas existentes tanto de la OTAN como financiados multinacionalmente. El conocimiento de la situación de los programas y a

incorporación de hitos facilitará el conocimiento y seguimiento del gap de capacidades.

Durante 2006-207 está previsto desarrollar programas detallados de trabajo para las áreas de capacidad específica, basados en perspectivas funcionales, tecnológicas o de servicios, que se denominarán CAIP,s.

El NNEC *roadmap* proporciona una priorización de el trabajo actual, planeado y futuro para llegar a obtener los atributos del futuro NNEC que haga operativas y eficientes las fuerzas de la Alianza.

La evolución promovida por la tranformación de las Fuerzas Armadas en la gestión de la información: el concepto NNEC y la revitalización de la ingeniería

Como consecuencia de la transformación los países están focalizándose en la evolución a NCW o NNEC (y se habla de *networked operations*, *network-based defense*, *network-generated capabilities*, etc.) y en una revitalización de las actividades técnicas y tecnológicas. Gran parte de la motivación inicial para esta revitalización proviene del análisis de las repercusiones que el abandono paulatino del rigor técnico estaba ocasionando, en el incumplimiento de los plazos de tiempo, y en un mayor coste del inicialmente estimado. Pero además la realidad ha mostrado la necesidad de no limitarse a hacer mejor las actividades habituales de ingeniería, sino a tener que redefinir los procesos y a desarrollar nuevas actividades técnicas.

Por lo tanto cómo consecuencia del proceso de transformación y la evolución a NEC surge la necesidad de una “nueva ingeniería”.

Es necesario ya para las Fuerzas Armadas tomar el paso de considerar el “diseño de servicios” frente al “diseño de productos”, a considerar las “especificaciones de capacidades y conceptos” frente a la “especificación de sistemas”, y a considerar la “prueba y validación de capacidades y sistemas de sistemas” frente a la “prueba de sistemas”. Es igualmente necesario pasar a considerar nuevos procesos como la”aceptación conjunta por un número n de usuarios”, “la medición de niveles de madurez tecnológica”, “las estimaciones integradas a nivel capacidad del coste total de propiedad”. Asimismo es necesario un nuevo apoyo a la toma de decisiones de

“modernizar frente a sustituir sistemas” , “de redimensionamiento de fuerzas y equipamiento”, etc.

La evolución a NNEC implica una nueva ingeniería enfocada a la definición de SOA,s, de sistemas de sistemas con la definición de nuevos estándares y técnicas y métricas de evaluación, etc.

No hay espacio en este capítulo del libro para explicitar la cobertura de esta “nueva ingeniería” en detalle por su extensión y complejidad. La realidad es que, además, en muchos puntos, no hay todavía procedimientos consolidados. Está ayudando mucho la voluntad de compartir esfuerzos para la aceleración de la puesta en marcha de NNEC por parte de gobiernos e industrias.

A la pregunta de quien puede proporcionar la capacidad de ingeniería necesaria para la evolución a NNEC, los países están contestando que únicamente la industria trabajando en entornos colaborativos. Siendo realistas el enfoque NEC transciende lo que las fuerzas armadas pueden desarrollar con su potencial humano. Este potencial es sin embargo crítico. La definición de conceptos es el gran demandante hoy en día de expertos de las Fuerzas Armadas en los países mas avanzados.

Se vive un mundo de contrastes. Se regulan los procedimientos para “el contratista acompañando a la fuerza” simultáneamente a que la definición y la validación de los sistemas requiera una contribución cada vez más significativa de los usuarios. La transformación ha abocado por lo tanto a una mayor interrelación Fuerzas Armadas con la industria.

Las empresas se están organizando en consorcios respondiendo al reto que marca la transformación y para posicionarse de cara al futuro. Así creen que están en mejor situación para poder asumir un compromiso de manera integrada y mejor poder aportar las ideas e iniciativas que hoy demandan las Fuerzas Armadas de terceras partes.

NCOIC (*Network Centric Operations Industry Consortium*) es el exponente claro de estas iniciativas. Creado en agosto de 2004, tenía ya en agosto de 2005, 80 organizaciones afiliadas. En la actualidad se acaba de producir la afiliación de la primera organización gubernamental: DISA (*Defense Information System Agency*).

Entre los integrantes de NCOIC se encuentran las principales empresas líderes en los sectores aeronáutico, espacio, tecnología de la información, etc, grandes integradores y empresas de servicios. El consorcio trabaja con clientes de todo el mundo y colabora con la OTAN, la Unión Europea y otras organizaciones.

Su objetivo es promover la aceleración del desarrollo e implantación de capacidades conectadas en red. Es clave pues para NCOIC el desarrollo de estandares y herramientas apropiadas para los marcos de arquitectura definidos por los países. La forma de trabajar es integrada con los clientes, y se pretende llegar a proporcionar un entorno centrado en red donde puedan operar toda clase de sistemas de información y se utilicen estandares abiertos, tanto consolidados como emergentes, en un marco global común bajo un mismo conjunto de principios y procesos.

El consorcio está dirigido por un director ejecutivo que reporta a un Consejo Ejecutivo y es asistido por una compañía de gestión (*The Open Group*). Hay dos grupos operativos además, un Consejo para temas de negocio y otro para temas técnicos, junto con un Consejo Asesor y otro Consejo afiliado.

Los grupos de trabajo son:

- El grupo de requerimientos del cliente. Define los requerimientos de las partes mediante un análisis de las arquitecturas establecidas por los organismos involucrados.

- El grupo de análisis de arquitecturas y estándares. Desarrolla un marco de arquitctura/modelo de referencia que identifica los estandares abiertos y su forma de utilización.

- El grupo de *building blocks*. Identifica el conjunto más amplio posible de producto desarrollados bajo los estandares abiertos.

- El grupo de educación y difusión. Proporciona un programa educativo para la diseminación de la información de NCOIC a través de las comunidades de tecnología de la información tanto militar como de la industria.

- El grupo de ingeniería de procesos. Planea y desarrolla estrategias de desarrollo de entornos colaborativos de ingeniería.

La citada agencia DISA (*Defense Information System Agency*) , recien incluida en NOIC acaba de publicar (octubre de 2006) unas líneas de acción estratégica para la industria (*Forecast* 2006) donde marca su visión del futuro. En esta se encuentra la consolidación del FDCE (*Federated Development and Certification En*vironment) consistente en un conjunto de procesos e infraestructuras para soportar las actividades de obtención de capacidades conectadas en red.

Otro consorcio relacionado con NCW es AFEI (*Association for Enterprise Integration*) que busca promover la colaboración entre organizaciones, la utilización de “mejores prácticas” , el intercambio de ideas en foros, etc.

Organismos gubernamentales e industria buscan por lo tanto la consolidación de proceso de ingeniería adaptados y generados para la construcción de la capacidad en red.

Los elementos de la gestión tecnológica:

los procesos y sus técnicas y herramientas

Para desarrollar la gestión tecnológica en el ámbito de las Fuerzas Armadas se han ido consolidando en el mundo una serie de actuaciones que a continuación se describen. Para realizar la gestión tecnológica, de manera similar que para acometer el “planeamiento por capacidades”, cada país tiene su propio proceso aún cuando los objetivos sean intrínsecamente los mismos. Hay que destacar que en cada caso los responsables de su Ministerio de Defensa han seleccionado y regulado la realización de un conjunto de actuaciones que configuran su forma de desarrollar su política tecnológica. Ninguna organización llega a contemplar la totalidad de los elementos que se enumeran a continuación, lo que probablemente sería inabordable desde el punto de vista de costes de gestión.

La selección, que premeditadamente o no realiza cada país, se lleva a cabo básicamente en función del modelo de ciclo de vida elegido en la gestión de sus adquisiciones, y del proceso de “aprobaciones” legislado por su organización. Por ejemplo el Reino Unido que utiliza el ciclo CADMID (concepto, evaluación,

demostración, fabricación, en servicio, retirada) y la aprobación a través de dos "puertas", tiene establecido por el AMS las herramienta y técnicas a utilizar por los IPT,S (*Integrated Program Teams*) en lo que respecta a la gestión tecnológica. Asimismo ha generado la matriz que indica lo que es necesario exigir en cada fase de un programa desde el punto de vista tecnológico y el nivel de madurez exigido a las tecnologías para pasar cada "puerta". Para medir el nivel de madurez ha establecido una escala de uno a nueve a través de la cual las tecnologías progresan según van adquiriendo un mayor nivel de madurez.

Las actuaciones pueden encuadrarse en tres grandes grupos: actuaciones a nivel de la organización y su forma de enfocar la gestión de adquisiciones y sistemas y la transformación de las Fuerzas Armadas y sus capacidades, actuaciones a nivel de conjunto de inversiones en modernización y mantenimiento, y actuaciones a nivel de programa, sistema o capacidad específica.

A continuación detallamos las actuaciones posibles en cada uno de estos tres niveles.

Las siguientes son algunas de las posibles actuaciones a realizar

a nivel de la organización y su proceso de transformación

DEFINICIÓN DE LA ESTRATEGIA TECNOLÓGICA DE LA ORGANIZACIÓN

Establece la polítca tecnológica de la organización y los medios y recursos para su desarrollo y el control del proceso. Por ejemplo la contenida en el Documento general ya citado del Reino Unido *Defence Industrial Strategy* en el que se indica para cada capacidad un enfoque tecnológico, o en el documento específico de la DPA (*Defence Procurement Agency*) *Technology Management Strategy*. Puede cubrir una parte solamente de la política estratégica como es el caso del Documento *International Science and Technology Strategy for the United States Department of Defense*.

GENERACIÓN DE UN *ROADMAP* DE LAS TECNOLOGÍAS DE LA ORGANIZACIÓN

Establece el camino para la evolución tecnológica de los medios de la organización, contemplando todos los elementos a considerar en el proceso a través del tiempo.

Es un ejemplo clásico el roadmap de UAV,s de Estados Unidos del cual se ha elaborado una segunda versión extendida en el tiempo.

GENERACIÓN DE PLANES ESPECÍFICOS DE INSERCIÓN DE TECNOLOGÍAS Y SUS CONSECUENCIAS (EN PERSONAL, INFRAESTRUCTURAS, ETC.)

Establece planes para poder conseguir de forma eficiente y bajo un nivel de riesgo controlado la incorporación de tecnologías nuevas o emergentes y las necesidades en términos de formación de personal o incremento del mismo, nuevo equipamiento,etc. El DoD ha publicado *The Manager Guide to Technology Transition in a Evolutionary Acquisition* que es un claro ejemplo, pues marca pautas y presenta lecciones aprendidas al respecto.

PUESTA EN MARCHA Y ACTIVIDADES DE UN SISTEMA DE OBSERVACIÓN TECNOLÓGICA

Genera una capacidad de identificar la situación tecnológica, las tecnologías emergentes y evaluar los programas de innovación tecnológica. Facilita la interrelación con organismos dedicados a la investigación y a la gestión tecnológica tanto a nivel nacional como internacional, incluyendo universidades, agencias, centros privados, etc y la interrelación con la industria. Facilita la integración y la difusión del conocimiento tecnológico. Los observatorios tecnológicos de la Subdirección de Tecnología y Centros de la Dirección General de Armamento y Material editan trimestralmente un *Boletín Tecnológico* de amplia difusión sobre el estado del arte de las tecnologías de la defensa.

DESARROLLO DE *WORKSHOPS* Y EJERCICIOS DE PROSPECTIVA TECNOLÓGICAS (AQUELLOS REALIZADOS FUERA DEL ÁMBITO DE LOS OBSERVATORIOS TECNOLÓGICOS)

Promueve la reflexión conjunta de los distintos participantes (todos los denominados *stakeholders*) con el fin de identificar las tecnologías emergentes y críticas, la demanda futura de tecnología, las oportunidades de cooperación y propone estrategias tecnológicas. La DPA del Reino Unido realiza eventos al respecto.

EVALUACIÓN DESDE EL PUNTO DE VISTA DE LA DEMANDA TECNOLÓGICA DE LOS ESCENARIOS OPERATIVOS

Analiza la demanda tecnológica de los escenarios operativos teniendo en cuenta que se han de soportar los requerimientos militares, proporcionando a las fuerzas capacidades militares de forma eficiente para su coste. Implica evaluar tanto las tecnologías que demandan el desarrollo de las misiones para contrarrestar las amenazas como las tecnologías que requieren las actuaciones que en el ámbito extenso de la seguridad realizan las Fuerzas Armadas. Dada la compartición de actuaciones con organismos gubernamentales no militares han surgido los conceptos de tecnologías duales, sistemas duales y capacidades duales. Así la demanda tecnológica de los escenarios es ya hoy en día en muchos casos compartida.

Por ejemplo el DoD y el Departamento de Homeland Security de Estados Unidos han desarrollado análisis sobre la demanda tecnológica para contrarrestar las acciones terroristas o la guerra urbana.

GESTIÓN DEL SISTEMA DE LABORATORIOS Y COORDINACIÓN

CON LAS REDES DE CENTROS Y LABORATORIOS INTERNACIONALES

Desarrolla la gestión de los laboratorios y centros de investigación dependientes del organismo de defensa responsable de la nación y desarrolla las actividades necesarias para coordinar el esfuerzo aplicado a nivel nacional con el realizado por otros países y organizaciones, de cara a compartir medios y generar planes comunes.

A nivel internacional las naciones están desarrollando acuerdos específicos bilaterales para temas concretos. Por ejemplo para las redes y la gestión de la información Reino Unido y Estados Unidos han creado la International Technology Alliance, y para las tecnologías de armas guiadas Reino Unido y Francia han creado la Innovation & Technology Partnership for Guided Weapons Technology. En ambas iniciativas participa la industria.

PUESTA EN MARCHA Y OPERACIÓN DE CENTROS DE VALIDACIÓN DE CONCEPTOS EN ENTORNOS COLABORATIVOS CON LA INDUSTRIA
Y EL PERSONAL OPERATIVO DE LAS FUERZAS ARMADAS

Plantea, diseña y pone en marcha centros de validación de conceptos. Desarrolla actividades de validación de conceptos ligados al proceso de transformación. Evalúa y valida las propuestas alternativas de soluciones para cubrir las carencias de

capacidades, considerando tecnologías emergentes y nuevos conceptos operativos. Estas actividades tienden a realizarse en el ámbito próximo a los responsables de la transformación, de la definición de estrategias militares y del planeamiento de capacidades concediendo la máxima importancia a la gestión de la información y los Sistemas C4ISTAR. Asimismo las validaciones de conceptos tienden a realizarse en entornos colaborativos con la industria y el personal operativo de las Fuerzas Armadas, pudiendo ser la industria la que proporcione las instalaciones o la que trabaje en cambio en instalaciones gubernamentales. Por ejemplo el TTCP (*The Technical Cooperation Program*) ha diseñado casos de validación de conceptos ligados a los procesos de transformación de las Fuerzas Armadas de los paises miembros y la DPA considera el uso de *Capability Concept Demonstrators*.

PUESTA EN MARCHA Y OPERACIÓN DE CENTROS DE DESARROLLO Y VALIDACIÓN DE DEMOSTRADORES TECNOLÓGICOS Y PROTOTIPOS OPERATIVOS EN ENTORNOS COLABORATIVOS CON LA INDUSTRIA Y EL PERSONAL OPERATIVO DE LAS FUERZAS ARMADAS

Plantea, diseña y pone en marcha centros de desarrollo y validación de demostradores tecnológicos y prototipos operativos. La evaluación y validación se facilita si se trabaja en entornos colaborativos ya que resulta indispensable la participación del usuario final. Estos entornos pueden ser propiedad de la industria, del organismo gubernamental responsable del proceso de la adquisición o del organismo del que dependan los usuarios finales. Hay ejemplos de las tres opciones en que se trabaja con pleno éxito, tanto en la validación de demostradotes tecnológicos como en la de prototipos operativos, y es una decisión a tomar como parte de la política de gestión tecnológica.

La DPA contempla la utilización de *Technology Demonstrators Programmes* para evaluar la aplicabilidad de las tecnologías. La LOI ha definido un Programa NECEP para la experimentación en NNEC para el desarrollo en un entorno colaborativo europeo de seis experimentos.

PUESTA EN MARCHA Y OPERACIÓN DE CENTROS DE PRUEBAS Y EVALUACIÓN DE SISTEMAS Y CAPACIDADES

Plantea, diseña y pone en marcha competencias de verificación,validación y pruebas, generando infraestructuras que permitan comprobar las prestaciones de los sistemas y su interoperabilidad en el entorno. Asimismo se trata de evaluar las

capacidades militares, buscando reproducir las condiciones que se presentarán en los escenarios reales. Hoy en día se planifica de manera integrada las pruebas y evaluaciones de todo el proceso incluida la aceptación. Por ejemplo: ITEA *Integrated Test Evaluation and Acceptance Planning* de Reino Unido.

Los entornos de V&V y pruebas de sistemas pueden ser propiedad de la industria, del organismo gubernamental responsable del proceso de la adquisición o del organismo del que dependan los usuarios finales, mientras que los entornos de V&V y pruebas de capacidades requieren siempre una fuerte participación multidisciplinar siendo terreno propicio para agrupaciones de empresas en colaboración con organismos gubernamentales. Por ejemplo desde hace años en el centro de entrenamiento y doctrina del Ejército de estadounidense (TRADOC) se ha trabajado en proyectos bajo contratos *ómnibus* en que participaban en las tareas: personal operativo, personal de las industrias, investigadores de las universidades, etc. Recientemente son empresas como Thales, Boeing, etc., las que han hecho el esfuerza en la creación de centros o agrupaciones como ITEA.

EVALUACIÓN TECNOLÓGICA DEL EQUIPAMIENTO DE LAS UNIDADES DE LA FUERZA Y EL SOPORTE A LA FUERZA

Permite analizar la adecuación tecnológica del equipamiento de las unidades de la fuerza y su ajuste con las misiones que previsiblemente deberán desarrollar. Resulta lógico que se realice ligada al proceso de transformación y sirve de *input* a los planes de obtención de tecnologías, con desarrollo de la priorización y la elaboración de roadmaps. La OTAN, ha través del RTO como organismo responsable de la investigación ha promovido proyectos de evaluación tecnológica del equipamiento de la fuerza. La LOI, por ejemplo, para el combatiente del futuro ha estudiado asimismo la armonización de requerimientos incluidos los aspectos tecnológicos.

EVALUACIÓN TECNOLÓGICA DE LAS CAPACIDADES MILITARES ACTUALES Y DE LA EVOLUCIÓN IMPLÍCITA EN EL PLANEAMIENTO DE CAPACIDADES

Permite evaluar la adecuación tecnológica de los medios actuales y previstos haciendo una lectura por capacidades. Su interés, respecto a la simple evaluación del inventario, radica en que se integra con la priorización de capacidades y facilita realizar la priorización de tecnologías. Esta es la forma actual de enfocar la

definición de la estrategia tecnológica por parte de los paises avanzados. Adicionalmente, como subproducto, se obtienen criterios para considerar la obsolescencia del material. Por ejemplo, puede establecerse la conveniencia de no focalizar inicialmente recursos en material de capacidades cuya cobertura y adecuación tecnológica sea adecuada o no sean capacidades prioritarias. El grupo de naciones TTCP (*The Technical Coordination Program*) citado anteriormente y formado por Australia, Canada, Estados Unidos, Nueva Zelanda y Reino Unido, ha analizado pautas para la realización de la evaluación tecnológica de capacidades.

VALORACIÓN ECONÓMICA DEL NIVEL DE ESFUERZO PARA LOGRAR

LA ADECUACIÓN TECNOLÓGICA LIGADO A LOS PROCESOS DE TRANSFORMACIÓN

Evalúa el coste de la modernización tecnológica del material ligado a los modelos alternativos evaluados en el proceso de transformación. Contempla tanto la modernización y upgrading como la sustitución o incorporación de nuevo equipamiento y el redimensionamiento necesario. Incluye los costes logísticos, de infraestructuras y entrenamiento del personal. Por ser muy complejo de calcular suele realizarse para análisis de casos particulares sirviendo como *input* en la toma de decisiones en los "*roadmaps* de transformación". Tras el proceso de *valuation* que están desarrollando en Estados Unidos, a finales de 2006, se espera disponer de datos y lecciones aprendidas. Para las decisiones de *upgrading versus* sustitución el DoD utiliza recientemente la metodología de la Rand Corporation.

EVALUACIÓN DE LA ADECUACIÓN DE LAS COMPETENCIAS/CAPACIDADES

EN MATERIA DE GESTIÓN TECNOLÓGICA DEL PERSONAL DE LA ORGANIZACIÓN

Evalúa la adecuación de las competencias/capacidades del personal considerando sus funciones actuales y las implicaciones de los cambios tecnológicos. Incluye la reorganización de puestos y niveles e igualmente la consideración del incremento o ajuste de plantillas. Diseña, valora, prioriza y desarrolla los planes de formación del personal controlando los resultados obtenidos. Los Ministerios de Defensa actualmente incluyen en sus planes de formación la competencia de gestión económica. La carrera profesional en la gestión de adquisiciones, por ejemplo el *acquisition stream* de Reino Unido, incluye un proceso secuencial de obtención de conocimientos de gestión tecnológica para desarrollar estas actividades.

Las siguientes actividades representan algunas de las posibles actuaciones de gestión tecnológica a realizar a nivel de conjunto de inversiones en modernización y mantenimiento de la organización. Buscando la brevedad no se incluyen referencias de ejemplos concretos, pero se han incluido aclaraciones en algunos casos

PLANIFICACIÓN GLOBAL DE PROGRAMAS DE INVESTIGACIÓN, DESARROLLO Y TECNOLOGÍA (I+D+T)

Establece la planificación de Programas de I+D+T permitiendo una lectura por área sectorial, por capacidad, por tipo de programa, por unidad usuaria, etc. Correlaciona con el presupuesto y establece los mecanismos de control. Presenta mecanismos de cofinanciación, cooperación con otros organismos, establecimiento de la propiedad intelectual, seguridad, etc. Contempla la interrelación con la industria a nivel diseño, prototipado, pruebas, etc y la aportación y propiedad de herramientas y medios.

PLANIFICACIÓN DE MODERNIZACIÓN TECNOLÓGICA A NIVEL SISTEMA DE SISTEMAS

Presenta para “sistemas de sistemas” (con particular énfasis en los sistemas de información) las pautas de actuación para una planificación coherente de modernización tecnológica de todos los sistemas “hijos”. Este proceso, surgido de la necesidad de coordinar la evolución de todas las parte de un sistema y garantizar su interoperabilidad en el tiempo, permite que la adquisición de las partes la realicen diferentes organismos. Puede decirse que es un proceso derivado del “control de interfaces” basado en que la tecnología representa una interfaz adicional y que en un sistema de sistemas hay que garantizar que exista una compatibilidad global a nivel tecnológico.

DEFINICIÓN DE LA ESTRATEGIA TECNOLÓGICA A TRAVÉS DEL CICLO DE VIDA

Establece las actuaciones y controles a realizar sobre los sistemas a través del ciclo de vida. Estas pautas son generales y enmarcan un contexto definido por los roles establecidos por la organización en la gestión tecnológica.

Definición y desarrollo de estrategias tecnológicas por sectores industriales

Plantea por parte de las Fuerzas Armadas la estrategia tecnológica por sector industrial. De reciente desarrollo, este mecanismo permite a los responsables de defensa transmitir a la industria su enfoque estratégico, indicando que tecnologías desean que el país posea y que por lo tanto están dispuestos a financiar a través de la adquisición de material de cuyo desarrollo formen parte. Respecto a la declaración de “tecnologías críticas” que el DoD lleva muchos años realizando, este proceso tiene la ventaja de que responde a una priorización resultante de la consideración del recurso económico y centra mejor el esfuerzo “recompensable” para las empresas.

DEFINICIÓN DE POLÍTICA DE OBSOLESCENCIA TECNOLÓGICA DEL MATERIAL

Establece por parte de los responsables de las Fuerzas Armadas la política de obsolescencia tecnológica, marcando las pautas a seguir en los procesos de obtención y mantenimiento. Recoge indicaciones sobre las claúsulas a incluir en los requerimientos y las garantias a obtener, de cara a asegurar la adecuación del nivel de madurez de las tecnologías, en los contratos. Establece los controles y evaluaciones a realizar y los análisis económicos para apoyar la toma de decisiones en materia de declaraciones de obsolescencia.

VALORACIÓN ECONÓMICA DEL NIVEL DE ESFUERZO PARA LOGRAR LA ADECUACIÓN TECNOLÓGICA DEL INVENTARIO DE SISTEMAS, DE LOS SISTEMAS DE UN SECTOR INDUSTRIAL, O DE LOS SISTEMAS AGRUPADOS EN FUNCIÓN DE SU NATURALEZA, OBJETIVO, ESTADO O ASIGNACIÓN

Evalúa el coste de adecuar tecnológicamente un conjunto de sistemas. En el caso del inventario global se suele analizar hoy en día capacidad por capacidad. En el caso de sistemas de un sector industrial se consideran los cambios tecnológicos inherentes al sector tanto en las tecnologías asociadas al diseño/desarrollo/fabricación como las asociadas al mantenimiento. Los países que analizan los costes del esfuerzo para la adecuación tecnlógica tratan de correlacionar las estimaciones resultantes con las estimaciones de incremento de efectividad. Un precursor de este tipo de análisis es la aplicación del COEIA (*Combined Operational Effectiveness and Investment Appraisal*) del AMS (Reino Unido) para el caso de mejoras tecnológicas.

Las siguientes son algunas de las posibles actuaciones a realizar a nivel de programa, sistema o capacidad específica.

Tampoco se han introducido ejemplos pero se han incluido algunos comentarios

EVALUACIÓN DE DISPONIBILIDAD DE UNA TECNOLOGÍA

Permite establecer para cada tecnología su nivel de posible utilización inmediata, en una escala que cubre desde el estado de desarrollo más incipiente de la tecnología hasta un estado en que su utilización en operaciones reales se ha constatado repetidamente. La escala más empleada hoy en día clasifica entre el nivel uno y el nivel nueve el estado de madurez alcanzado por una tecnología. Algunos países establecen los niveles de madurez exigibles a las tecnologías críticas de los proyectos a demostrar en los hitos del calendario de desarrollo de los mismos.

EVALUACIÓN DE LA ADECUACIÓN DESDE EL PUNTO DE VISTA TECNOLÓGICO DE LA OBTENCIÓN DE UN SISTEMA

Permite establecer el riesgo desde el punto de vista tecnológico del sistema considerando los riesgos de las tecnologías implicadas junto con los riesgos asociados a su integración.

EVALUACIÓN DESDE EL PUNTO DE VISTA TECNOLÓGICO DE UN PROYECTO

Permite establecer el avance global en madurez de un proyecto basado en la situación de las áreas o disciplinas básicas: avance técnico, entrenamiento, seguridad, fiabilidad, sistemas de información y comunicaciones, interfaces, etc.

Se suele establecer una matriz de correlación de la evolución a través de las correspondientes fases del proyecto con los logros a alcanzar en cada área. La situación de las áreas muestra el avance conseguido. Por ejemplo comprobación previa a “la puesta en servicio” de que el resultado de las pruebas de fiabilidad de un elemento de nuevo desarrollo del proyecto es correcto.

EVALUACIÓN DE RIESGOS TECNOLÓGICOS LIGADOS A LA OBTENCIÓN DE UNA CAPACIDAD

Permite evaluar los riesgos asociados a la obtención de cada uno de los elementos de una capacidad. Por ejemplo necesidad de reciclar al personal en la utilización y mantenimiento de un sistema modernizado.

GENERACIÓN DE DICTAMEN DE RIESGO DE OBSOLESCENCIA TECNOLÓGICA DE UN SISTEMA

Permite evaluar los riesgos de que un sistema se quede obsoleto antes de la fecha prevista para su sustitución o modernización.

VALORACIÓN ECONÓMICA DEL NIVEL DE ESFUERZO PARA LOGRAR

LA ADECUACIÓN TECNOLÓGICA A NIVEL PROGRAMA, SISTEMA O CAPACIDAD

Evalúa el coste para adecuar el estado tecnológico a lo requerido en cada caso.

Iniciativas emergentes en la gestión tecnológica

de los sistemas de información

Para los sistemas de información han surgido en los últimos años una serie de iniciativas en gestión tecnológica, desarrollando algunos de los elementos descritos en el apartado anterior. Han sido generadas a partir de la percepción de que es necesario dar a las Fuerzas Armadas el sistema de sistemas que necesitan y no un conjunto de sistemas desarrollados, adquiridos e utilizados de manera inconexa.

Respecto al planeamiento:

- Todos los países están haciendo la tarea de reevaluar sus grandes planes de obtención de sistemas de información, y en particular NEC se ha adoptado como objetivo y como tecnología.

- Como consecuencia de haber participado en el estudio de viabilidad sobre NEC realizado por OTAN o de análisis propios las naciones han definido, con mayor o menor concreción, una postura nacional sobre NEC.

- Se está en camino de generalizar la elaboración de roadmaps sobre NEC. Los ejemplos del *NATO NNEC roadmap* publicado el 3 de julio de 2006 o la revisión del roadmap sobre NNEC del gobierno australiano son muestras de definición de

objetivos, tareas, marcos temporales y asignación de responsabilidades en la implantación de NNEC.

- Se está trabajando asimismo en una perspectiva a 2010 y a 2020. En la primera las naciones y organismos se centran básicamente en la búsqueda de la efectividad y de la interoperabilidad. Por ejemplo AIS (*The Bi-SC Automated Information Systems strategy 2005-2010*) de OTAN publicada el 19 de junio de 2006. Para el 2020 se están elaborando futuras visiones de capacidades y escenarios NNEC en los que existan estrategias a nivel capacidades. Por ejemplo para los Sistemas ISTAR, con medios comunes a nivel OTAN o Unión Europea para garantizar la interoperabilidad del pool de medios.

Respecto a la definición de conceptos:

- En la definición de conceptos se está avanzando, bien a través de la puesta en marcha de laboratorios de validación de conceptos, bien con ejercicios de armonización de requisitos entre naciones, bien con análisis generados como soporte del proceso de transformación. El TTCP constituido por varios países. ha publicado una guía para la realización de experimentación (GUIDEX) a la vez que organiza seminarios orientados a compartir experiencias en el planeamiento por capacidades. La LOI ha lanzado un plan de experimentación en NNEC que servirá para validar conceptos resultantes de los procesos de transformación de las naciones miembros.

- Para identificar las tecnologías que precisan una inversión de cara a una demostración de su adecuación se está aplicando ITAP (*Integrated Tecnology Acquisitions Plans*) según el proceso del AMS (*Acquisition Management System*) del Reino Unido, Esta demostración se considera que debe hacerse simultáneamente a la definición de conceptos indicada, para tener la tecnología apropiada disponible en el momento oportuno. El ITAP es un proceso iterativo consistente en cuatro subprocesos: definir/revisar requerimientos clave (procedentes de las necesidades del usuario), definir/ revisar objetivos de conocimiento, definir/revisar planes tecnológicos y definir/revisar programas de demostración de tecnologías.

- Para facilitar la toma de decisión, basada en información adecuada, por parte de un entorno múltiple de usuarios se están desarrollando metodologías específicas. E-DEL+I es una técnica analítica de la Rand Corporation que establece el marco y el proceso de la toma de decisión.

Respecto a la validación de interoperabilidad de sistemas de sistemas:

- Con respecto a los enfoques de evaluación de interoperabilidad hay hoy en día varios procedimientos en uso en estado más o menos incipiente:
  - El procedimiento LISI (*Levels of Information System Interoperability*).
  - El procedimiento JITC (*Compliance Testing*).
  - El *Report on Interoperability* de la OTAN NIAG (*Industrial Advisory Group*).
  - La evaluación *Net-ready* KPP (*Key Performance Parameters*).

Respecto a la validación y pruebas de capacidades y sistemas de sistemas:

- Respecto a la validación y pruebas de sistemas hay que decir que es sin duda uno de los campos donde más se ha avanzado. El progreso resulta comparable a los experimentados por las evaluaciones económicas o la nueva logística, que transcienden el ámbito de esta *Monografía*.
- Se está extendiendo la tendencia definida como ITEA del AMS del Reino Unido a la vez que ha surgido como un nuevo campo de trabajo la prueba y evaluación de capacidades. Esta función se distancia del mero campo tecnico, al no poder realizarse en los centros de prueba clásicos, y de la dependencia exclusiva de un ejército, y se acerca al organismo responsables del diseño de la transformación y el planeamiento de la gestión de la información. Un ejemplo de pruebas basadas en capacidades son las actividades realizadas por el Cuerpo de los *Marines* estadounidenses utilizando las directrices del MCOTEA Guidebook for Capabilities-Based Testing.
- Para la evaluación de los sistemas y las tecnologías de la información y los sistemas NCW o NNEC existen hoy mecanismos y métodos de muy reciente

utilización. Estos métodos no son comunes, a semejanza de lo que ocurre con el planeamiento por capacidades.

- En Estados Unidos se utiliza la evaluación *Net-ready* considerando los denominados *Key Performance Parameters*. Esta es una evaluación de cumplimiento basada en el comportamiento y las prestaciones contra una arquitectura definida y un conjunto de estándares y directrices. Los elementos para determinar el cumplimiento, declarando *Net-ready* a un sistema y procediendo a su certificación en el entorno del DoD son:

  - Cumplimiento del modelo de referencia para *Net Centric Operations and Warfare Referente Model*. En particular se mira el cumplimiento respecto a conceptos, procesos, servicios, estandares, lenguaje y taxonomía.

  - Cumplimiento con el marco de la arquitectura (DODAF).

  - Consideración de las interfaces.

  - Acreditación de seguridad de la información IA (*Information Assurance*).

  Como referencia está el report preparado por el *Operacional Test Agency Commander´s Net-Ready Performance Study Group* sobre *Net-Ready Key Performance Parameter*.

- En el Reino Unido las evaluaciones de NNEC se centran todavía más en su justificación más que en la certificación de sistemas para ser incorporados. Para evaluar NNEC se utiliza el *Network-enabled Capability Benefit Análisis* consistente en un análisis que busca entender la relación entre las inversiones relacionadas con NNEC y la efectividad de la fuerza. Se está haciendo igualmente un esfuerzo en la definición de métricas y en los estudios sobre el balance de inversiones de sistemas *hard* respecto a los sistemas de información.

- En los países escandinavos se utiliza el NBD (*Network-based Defence*) análisis para identificar la relación entre la capacidad en red y la efectividad de la fuerza.

- En Australia se utiliza la metodología NPI. Su enfoque consiste en un análisis sistema a sistema para evaluar en qué grado los proyectos bajo construcción y las

capacidades en introducción son capaces de integrarse y contribuir a la capacidad en red.

Respecto a la posición de la industria:

- Hay que resaltar dos grandes líneas de acción: el cambio en la interrelación defensa-industria y la generación de plataformas industriales orientadas a NEC como sistemas de sistemas.

- En la primera línea se incluyen las iniciativas para exponer más claramente los requisitos de la administración, los nuevos proceso de contratación y la puesta en marcha de entornos colaborativos. Son ejemplos: la citada metodología MODAF (*The Ministry of Defence Architectural Framework*) del Reino Unido que facilita expresar los requerimientos NNEC y establecer arquitecturas consistentes en todo el ámbito del Ministerio de Defensa, o su equivalente arquitectura DODAF en USA, los procesos SBIR de contratación en el marco Estados Unidos con documentación simplificada y recepción de *white papers* con propuestas de industrias emprendedoras, y los múltiples foros conjuntos Administración-industria para establecer estrategias en el desarrollo NNEC.

- Existen ejemplos claros de iniciativas en el campo NNEC. Por ejemplo Boeing y QneticQ quieren expandir sus capacidades de *network-enabled* mediante la operación de un centro para colaboración y experimentación. En este centro se ofrecerá a los usuarios la modelización, la simulación y herramientas de análisis para explorar y comprender las implicacines de los sistemas propuestos en un entorno dinámico de tiempo real.

- Asimismo Thales ha creado el *Battlefield Transformation Centre* para evaluar los conceptos propuestos por el usuario.

- Respecto a la formación de plataformas industriales hay que resaltar tanto la formación de grandes plataformas como el NCOIC (*Network Centric Operations Industry Consortium*), como la generación de grupos específicamente para un contrato determinado.

- Las grandes plataformas se crean para fortalecer un área tecnológica creando una infraestructura industrial capaz de acometer el diseño, desarrollo, puesta en operación y soporte a la operación de sistemas de sistemas. El consorcio NCOIC integra a las principales empresas de nivel internacional y es un motor para NNEC. Una ventaja que tienen estas plataformas es la mayor facilidad en la adopción de estandares, la mayor garantía de interoperabilidad, un mejor control de interfaces, costes, y una garantía de cara a la evolución del sistema de sistemas, sistemas, subsistemas y componentes.

- Otras veces se crean asociaciones para desarrollar un aspecto concreto como pueden ser las pruebas o las certificaciones de seguridad. Por ejemplo ITEA.

- A nivel nacional hay una propuesta generada por INDRA, EADS-Casa, GMV y SENER para trabajar para la LOI/EDA en el entorno NEC.

Consideraciones generales:

Una vez expuestas estas iniciativas emergentes es el momento de hacer una reflexión.

En España quedan dos asignaturas pendientes para la industria:

- Incrementar la participación en NNEC a nivel internacional (NNEC, EDA, etc.).

- Integrar un grupo industrial “completo” que se pueda hacer cargo del desarrollo del futuro NNEC nacional a partir del SMCM y los Sistemas LEGACY y sea capaz de generar propuestas atractivas a las Fuerzas Armadas. Si existiese voluntad, de un número significativo o al menos de un núcleo inicial de empresas, se podría lanzar una iniciativa de coordinación de una plataforma NNEC, para comenzar pronto la definición de su estructura y la generación de propuestas. Eso sería posible, dado que la matriz de capacidades técnicas y el arbol de tecnologías (al estilo francés) para desarrollar el futuro Sistema NNEC están bastante claros, siempre que se adoptase una postura proactiva y enfocada al posicionamento favorable para todas las partes.

  El alcance inicial podría ser más o menos ambicioso así cómo el enfoque final. Se puede concebir un proceso evolutivo, con un alcance limitado inicialmente a

los sistemas C-4ISTAR de las Fuerzas Armadas, hasta llegar a considerar un enfoque para cubrir el entorno de seguridad nacional, o un NNEC para las Fuerzas Armadas que integre el equivalente al *sense and respond logistic*.

Es importante resaltar dos cosas. La primera es que un retraso en el planteamiento de iniciativas NNEC puede conllevar una clara pérdida de oportunidades a las empresas españolas y filiales españolas de empresas internacionales, dado que las empresas internacionales madres claramente están posicionándose. La segunda es la posibilidad clara, en línea de otros países de que NNEC pueda ser considerado una iniciativa de I+T a nivel nacional, y en consecuencia tener abiertas las líneas de financiación existentes y posibles en un futuro próximo

El interés y la conveniencia para los Ministerios de Defensa de que surjan estas iniciativas es innegable ya que la puesta en marcha de un sistema de sistemas para la gestión de la información requiere niveles de coordinación inalcanzables sin estas iniciativas. No son suficientes los esfuerzos industriales si las administraciones no hacen sus tareas y elaboran las estrategias y directrices necesarias; pero la complejidad de los sistemas de sistemas trasciende en mucho el nivel de esfuerzo que puede realizar la Administración o una empresa aislada y requiere soluciones imaginativas en las que todas las partes resulten ganadoras.

La gestión tecnológica en las Fuerzas Armadas españolas

Habiéndose descrito en otros capítulos del libro las necesidades tecnológicas de nuestras Fuerzas Armadas y el plan de investigación y desarrollo del Ministerio de Defensa mencionaremos aquí de forma muy breve, solamente las actividades de gestión tecnológica, sin detenernos en las tecnologías, salvo una somera referencia a las actuaciones relativas a NNEC

Las Fuerzas Armadas españolas han venido realizando actividades de gestión tecnológica desde hace más de dos décadas, si bien ha sido en los últimos diez años cuando se ha consolidado por la Subdirección General de Tecnología y Centros (SDGTECEN) de la Dirección General de Armamento y Material (DGAM) un planeamiento sólido de programas de I+D y una incorporación significativa a los programas internacionales.

Asimismo la SDGTECEN ha puesto en marcha y desarrolla las funciones propias de un sistema de observación tecnológica mediante un conjunto de observatorios tecnológicos que proporcionan a las Fuerzas Armadas el conocimiento del estado del arte de las tecnologías de su interés, a la vez que facilitan a la DGAM la elaboración de informes de apoyo a la toma de decisión en los hitos propios de los desarrollos de los programas. La SDGTECEN cuenta con centros donde se desarrollan actividades de investigación y controla los desarrollos tecnológicos, en forma de demostradores tecnológicos, prototipos operativos e incluso preseries que desarrolla la industria. En particular respecto a NEC la SDGTECEN ha venido generando en el Polígono de Experiencia de Carabanchel un demostrador tecnológico de interoperabilidad de Sistemas CIS.

El Estado Mayor de la Defensa (EMAD) como organismo al que pertenecen el Mando de Operaciones, el de Transformación, la División CIS y la División de Estrategia y Planes es el organismo que integra las competencias de planeamiento de capacidades definición del proceso de transformación y planificación e implantación del Sistema de Mando y Control Militar (SMCM) a la vez que participa como responsable en los órganos a nivel OTAN y Unión Europea que coordinan las actividades CIS. Respecto a NEC la división CIS es la responsable tanto de las actividades de definición de la necesidad operativa, como de la participación en iniciativas como el análisis de viabilidad NEC de OTAN.

La Inspección General CIS (IGECIS), como responsable del Plan Director CIS, con respecto al SMCM ha venido trabajando en el desarrollo del marco de arquitectura, colaborando con la División CIS del EMAD, y en el desarrollo de los Subsistemas del SMCM, para entregárselos a la División CIS para su implantación. Su labor ha sido fundamental hasta la fecha para el avance del SMCM, habiendo canalizado fondos de I+D para posibilitar el desarrollo de la COP y otros logros.

Analizando las funciones que surgen para el desarrollo del futuro NNEC nacional y la participación en las iniciativas OTAN parece evidente la necesidad de una planificación a realizar desde la División CIS que podrá evaluar las implicaciones en términos técnicos y económicos de las alternativas de la capacidad C4ISTAR para cubrir los requerimientos del Mando de Operaciones y las directrices para la Transformación. Igualmente parece evidente que es la División CIS el organismo

que siguiendo las nuevas pautas de validación de capacidades debería ser en el futuro el que validase la capacidad C4ISTAR. Hay que destacar la necesidad de la participación de los operativos y responsables de los sistemas tácticos que representan la realidad actual (los sistemas que en el futuro constituirán el conjunto de sistemas legacy). Dada la realidad presupuestaria la problemática de una evolución financiable impondrá caso a caso la estrategia de evolución específica.

En caso de que a nivel nacional se consolidase como parece conveniente un grupo industrial ligado al desarrollo NNEC parecería lógico que interaccionase con la División CIS del EMAD en los requerimientos operativos del NNEC y la verificación y validación del sistema y comprobación de la obtención de la capacidad.

Los retos para la gestión tecnológica

de los sistemas de información de las Fuerzas Armadas en España

Para las Fuerza Armadas españolas el proceso de transformación y la evolución a NNEC connlleva unos retos ligados al desarrollo de la gestión tecnológica:

- Impulsar una política de gestión tecnológica, generando a semejanza del Reino Unido y otros países documento avanzados una estrategia industrial y tecnológica ligada a las capacidades.
- Reforzar el planeamiento de capacidades con implicaciones tecnológicas.
- Impulsar la definición de una arquitectura C4ISTAR (ampliando la arquitectura C3 actualmente definida).
- Consolidar y difundir el concepto de GIG nacional.
- Generar un enfoque de escenario 2020 para C4ISTAR evaluando recursos y tecnologías.
- Potenciar la planificación NNEC desde el EMAD elaborando un roadmap NNEC y un marco de implantación NNEC.
- Coordinar el esfuerzo nacional con NNEC y las iniciativas a nivel de la EDA.

- Poner en marcha un laboratorio de validación de conceptos ligado al proceso de Transformación y al Mando de Operaciones.

- Poner en marcha un laboratorio de desarrollo de demostradores tecnológicos y prototipos en el futuro ITM (o centro alternativo de la propia SDGTECEN) o bien colaborar con la industria en las instalaciones de esta con soporte de usuarios (operativos y técnicos).

- Generar un concepto de "evaluación *net-ready*", que, por ejemplo, podría implementarse a partir de una evolución del grupo de análisis de vulnerabilidades (INFOSEC) del EMAD.

- Participar con la industria en un entorno colaborativo de pruebas apoyando con usuarios la pruebas operativas, participando en las pruebas técnicas y desarrollando el proceso de validación *net-ready*.

- Reforzar la coordinación con la industria de cara a la EDA y otros organismos.

- Formar personal de las fuerzas armadas y de la industria en gestión tecnológica con conocimiento específico para la inserción tecnológica.

- Apoyar mediante *coaching* a los responsables en el ámbito NEC fomentando una visión estratégica y global.

- Generar un sistema de métricas proporcionando visibilidad sobre los programas en curso, las iniciativas en el entorno NNEC y la situación relativa respecto a otros entornos a los responsables de las Fuerzas Armadas.

Bibliografía

A continuación se enumeran cómo referencia un subconjunto de las fuentes bibliográficas estudiadas para confeccionar el capítulo.

Defence Industrial Strategy White Paper. Diciembre 2005. Ministry of Defence. UK.
Enabling Acquisition Change. Junio 2006. Ministry of Defence. UK.
Defence Technology Strategy for the demands of the 21st century. Octubre 2006. Ministry of Defence. UK.
Network Enabled Capability. JSP777. 2005.Ministry of Defence. UK.
Operations Analysis Support to Network Centric Operations - UK Overview. 2004. Defence Science and Technology Laboratory[dstl].UK.

Defense Acquisition Performance Report. DAPA. Enero 2006. USA
The Implementation of Network-Centric Warfare. 2005. Office of Force Transformation. Office of the Secretary of Defense. USA.
Network Centric Warfare: Background and Oversight Issues for Congress. 2005. The Library of Congress. USA.
Net-Ready Key Performance Parameter (NR-KPP) Study Report. 2005. Operational Test Agencies (OTA). USA
International Science and Technology Strategy for the United States Department of Defense. Abril 2005. Department of Defense. Defense Research & Engineering. USA.
Le Plan Prospectif a 30 Ans. Annexe : Tableaux Récapitulatifs de la Prospective des Systèmes de Forces. Mayo 2005. Délégation Générale pour lÁrmement. France.
Forum 2006 “Opérations en réseau ». Module 5 : Prise en compte du contexte international.10 Octubre 2006. Délégation Générale pour lÁrmement. France.
NCOIC website : www.ncoic.org.
Network Centric Operations Industry Consortium Panel. Marzo 2006. NCOIC.
NCOIC White Paper. Julio 2005. The MITRE Corporation.
2006 Annual ITEA Technology Review. 7-10 Abril 2006. International Test and Evaluation Association.
Network-Centric Operations: European Capabilities. Document A/1899. Junio 2005. WEU
NEC Challenges and their impact on networking technologies. Abril 2006. R&T Directorate. European Defence Agency. EDA.
Development of a NATO Network Enabled Capability (NNEC). MCM-0038-2005. NATO.
NNEC Feasibilty Study Version 2.0. Octubre 2005. NATO.
NATO Network-Enabled Capability (NNEC). Roadmap. Junio 2006. ACT. NATO.

EPÍLOGO

EPÍLOGO

Por ÁNGEL MONTOYA CEREZO

A pesar de cambiar los escenarios, los potenciales enemigos y los tiempos, la tecnología aplicada o nacida en el ámbito militar ha sido y es motor del desarrollo de nuevas aplicaciones que han revolucionado cada época.

Internet es uno de los últimos paradigmas del uso de una tecnología nacida como exclusivamente militar y que ha evolucionado como aplicación civil extendida a todo el planeta. Sus precursores no eran conscientes del alcance que significaba ni somos hoy día adivinos de la evolución que puede tener.

Los sistemas de posicionamiento como el GPS, conducen a aplicaciones como la gestión de flotas, los sistemas de rescate, de posicionamiento para alejamientos judiciales, montañeros, servicios de telealarma en taxis, etc.

A partir de los Sistemas de Control y Vigilancia de Costas aparece el control de las aguas jurisdiccionales, control de tráfico de estupefacientes, contrabando, inmigración ilegal, etc. Los sistemas de radar aplicados al control de tráfico aéreo en vuelo y en superficie regulan el transporte aéreo mundial. Desde los centros de mando y control militares se desarrollan los sistemas de atención de emergencias, tipo 112, con gestión de incidencias, gestión de recursos, seguimiento de móviles, despliegues de medios de emergencia, etc.

Al contrario, los estamentos militares utilizan sistemas civiles para su servicio, como redes informáticas, software comercial, telefonía fija y móvil, videoconferencia, comunicaciones por satélite, etc. Sistemas de giroestabilización desarrollados inicialmente para plataformas, sistemas militares y de uso en cámaras de retransmisión de eventos televisados. Sistemas de cifrado con algoritmos hoy usados en vida civil . Todo ello no hace más que confirmar el fenómeno de la dualidad de tecnologías.

En el año 1958 se crea en Estados Unidos la Agencia de Proyectos Avanzados de Investigación (ARPA), que luego pasaría a llamarse DARPA, al objeto de dotar a su Departamento de Defensa de las más altas capacidades tecnológicas formulando y ejecutando los proyectos de Investigación y Desarrollo (I+D) que puedan darle la supremacía. Resultado de sus trabajos, quizás el éxito mas popular, fue la red ARPANET precursora de Internet. Esta Agencia pretende adelantándose a los requerimientos futuros que le permitan explotar la tecnología con éxito, trabajando en disciplinas que cubren los requisitos de la defensa y de la seguridad nacional. Recientemente se ha concentrado en proyectos esencialmente exploratorios y de investigación básica.

Desde Europa, la atomización de presupuestos de Defensa y la discrepancia de intereses nacionales, dificulta la armonización de planes tecnológicos, incluso para otras áreas de aplicación distinta a la defensa. Mientras no cambie este criterio, será importante la implicación de los organismos estatales de forma individual.

En paralelo, la industria seguirá desarrollando tecnologías que le permitan cubrir todos los mercados, incluido naturalmente el de defensa. Ambas, industria y administraciones nacionales, han de buscar la optimización de los presupuestos e inversiones en desarrollo de tecnologías, unos como administradores de los recursos de los estados y otros como generadores de beneficios empresariales.

Confiamos que con este trabajo se aporte una visión clara de la situación actual y los campos de interés para el futuro.

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

AEN	All Encrypted Network
AM	Amplitud Modulada
ATM	Asynchronous Transfer Mode
AWACS	Airborne Warning and Control System
BCN	Black Core Network
BLOS	Beyond Line of Sight
BMD	Ballistic Missile Defense
CAS	Close Air Support
CECEA	Centro Corporativo de Explotación y Apoyo
CG	Cuartel General
CGS	Centro de Gestión del Sistema
CIMIC	Civil-Military Cooperation
CIS	Communication and Information Systems
CNI	Centro Nacional de Inteligencia
COMINT	Communications Intelligence
COP	Common Operational Picture
COTS	Commercial On The Shelf
C2	Command and Contol

C3	Command, Control and Communications
C3I	Command, Control, Communications and Intelligence
C4	Command, Control, Communications and Computers
C4ISR	Command, Control, Communications, Computers, Information, Surveillance and Reconnaissance
DAMA	Satellite Demand Assigned Multiple Access
DEW	Directed-energy Weapon
DF	Direction Finding
DSP	Digital Signal Processor
ECM	Electronic Counter-Measures
ECCM	Electronic counter-countermeasures
ELINT	Electronic Intelligence
EM	Estado Mayor
EMAD	Estado Mayor de la Defensa
ENIAC	Electronic Numerical Integrator and Calculator
EPM	Electronic Protective Measures
ERINT	Extended Range Interceptor
ERIS	Exoatmospheric Reentry-vehicle Interceptio System
ESM	Electronic Support Measures

EW	Electronic Warfare
FAS	Fuerzas Armadas
FFT	Friendly Forces Traking
FLAGE	Flexible Lightweight Agile Guided Experiment
FLIR	Forward Looking Infra Red
FM	Frecuencia Modulada
FO	Fibra Óptica
FPGA	Field Programmable Gate Array
GBS	Global Broadcasting System
GPRS	General Packet Radio Service
GPS	Global Positionning System
GSM	Global System for Mobile Communications
Gw	Gateway
HF	High Frecuency (3-30 Mhz)
HOE	Homing Overlay Experiment
HUMINT	Human Intelligence
HW	Hardware
INFOSEC	Information Security
ICBM	Inter Continental Ballistic Missiles

IP	Internet Protocol
IRBM	Intermediate Range Ballistic Missile
ISDN	Integrated Services Digital Network
ISR	Intelligence, Surveillance and Reconnaissance
IW	Information Warfare
JCE	JAVA Cryptography Extension
J2EE	Java 2 Enterprise Edition
LAN	Local Area Network
LOS	Line of Sight
MAD	Mutual Assured Destruction
MANET	Mobile Area Networks
MINISDEF	Ministerio de Defensa
MIP	Multilateral Interoperability Program
MIRV	Multiple Independently Targetable Reentry Vehicle
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NCW	Network Centric Warfare
NNEC	NATO Network Enable Capability
NTBT	Nuclear Test Ban Treaty

OI	Organización Internacional
ONG	Organización No Gubernamental
PC	Post of Command
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
POTS	Plain Old Telephony System
P&P	Plug and Play (Sistema de conexion automática “Conecta y Funciona”)
QoS	Quality of Service
RADAR	Radio Direction and Ranging
RBA	Red Básica de Área
RCT	Red Conjunta de Telecomunicaciones
RDSI	Red Digital de Servicios Integrados
RDSI-BRI	Red Digital de Servicios Integrados. Acceso Básico (2B+D) B=64 Kbps, D=16 Kbps)
RDSI-PRI	Red Digital de Servicios Integrados. Acceso Primario (Europa: 30B+D) B=64 Kbps, D=64 Kbps, 1 Canal de 64 Kbps sincronía)
RFID	Radio Frecuency Identification
RGT	Red Global de Telecomunicaciones
RLP	Recognised Land Picture

RMA	Revolution in Military Affairs
RPV	Remotely Piloted Vehicles/Red Privada Virtual
SA	Situation Awareness
SADIESFAS	Sistema de Planeamiento, Gestión y Evaluación del Adiestramiento y Preparación de la Fuerza.
SALT	Strategic Arms Limitation Treaties
SCTM	Sistema Conjunto de Telecomunicaciones Militares
SCUD	
SDH	Synchronous Digital Hierarchy
SDI	Strategic Defense Initiative
SDR	Software Defined Radio
SECOMSAT	Sistema Español de Comunicaciones por Satélite
SHF	Super High Frecuency (3-30 Ghz)
SI	Sistemas de Información
SIAOT	Sistema de Información de Apoyo a las Operaciones Terrestres
SICAMOFAS	Sistema de Gestión Cartográfica, Meteorológica y Oceanográfica de las Fuerzas Armadas
SICISFAS	Sistema de Gestión de Apoyo CIS a las Operaciones
SIDOCFAS	Sistema de Gestión y Difusión de la Doctrina de las Fuerzas Armadas

SIECOMFAS	Sistema de Estrategia y Cooperación Militar de las Fuerzas Armadas
SIGINT	Signals Intelligence
SILOGFAS	Sistema de Gestión y Coordinación Logística de Operaciones de las Fuerzas Armadas
SIMENFAS	Sistema de Mensajería Militar
SINTEFAS	Sistema de Inteligencia de las Fuerzas Armadas
SIOPERFAS	Sistema de Apoyo a la Conducción de Operaciones
SIPLAFAS	Sistema de Planeamiento de las Fuerzas Armadas
SIVIDEOFAS	Sistema de Videoconferencia Militar
SMCM	Sistema de Mando y Control Militar
SOA	Services Oriented Architecture
SOAP	Simple Object Access Protocol
SW	Software
TACOMSPOST	Tactical Communications Post
TDMA	Time Division Multiple Access
TLC	Low Temperature Cofired Ceramics
UAV	Unmanned Air Vehicle
UDDI	Universal Description, Discovery and Integration
UHF	Ultra High Frecuency (300 Mhz-3 Ghz)

VHF	Very High Frecuency (30-300 Mhz)
WAN	Wide Area Network
WAP	Wireless Application Protocol
WIFI	Wireless Fidelity
WIMAX	Worlwide Interoperability for Microwave Access
WML	Wireless Markup Language
WS	Web Sevices
WSDL	Web Services Description Language
XML	X-Tensible Markup Language

COMPOSICIÓN DEL GRUPO DE TRABAJO

Presidente D. ÁNGEL MONTOYA CEREZO
Director del Área de Defensa y Fuerzas de Seguridad de TECOSA (Grupo SIEMENS)

Coordinador D. JUAN ORTI PÉREZ
Coronel de Infantería de Marina
Máster en Paz, Seguridad y Defensa por el Instituto Universitario "General Gutiérrez Mellado".

Vocales D. TOMÁS FERRÁNDEZ ARAGÜES
General de Brigada del Ejército de Tierra
Subdirector de los Sistemas de Información y Telecomunicaciones del Ejército de Tierra.

Dª CLEMENTINA BRAVO PÉREZ
Doctor en Ciencias Físicas Consultora.

Dª SILVIA SORIANO ARÉVALO
Directora de Defensa. SUN Microsystems Ibérica.

D. ENRIQUE HERRERA CORTÉS
Teniente Coronel del Ejército de Tierra
Profesor de la ESFAS (CESEDEN).