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.

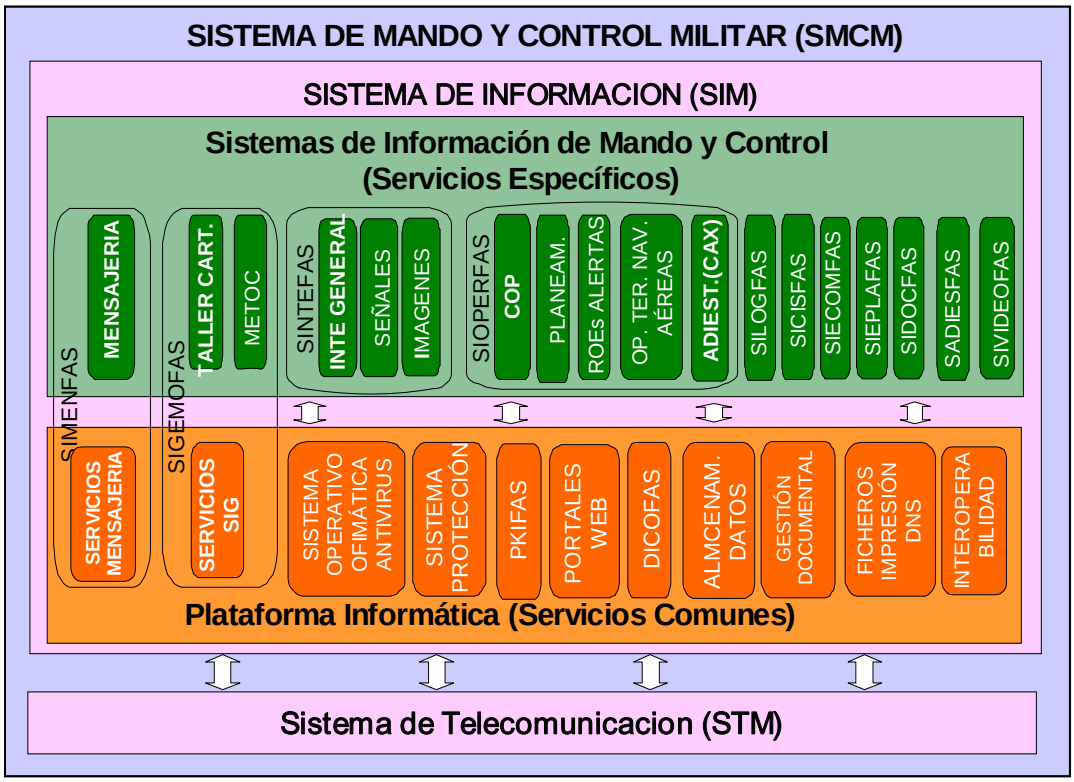
En cuanto a los Sistemas de Información en el ámbito del Ministerio de Defensa, la situación actual viene impuesta por el Plan de Obtención y Modernización de los Sistemas de Información de Defensa. En lo que al área de mando y control se refiere, se está realizando la definición del Sistema de Mando 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