El Plan Director CIS ha sabido anticiparse a las necesidades que supondría el desarrollo exponencial de las TIC, planificando y desarrollando con antelación las soluciones más adecuadas

General del Aire Jefe de Estado Mayor de la Defensa

entrevista realizada por Jesús Rivero Presidente de DINTEL

y editor de la revista

Dintel ALTA DIRECCIÓN

fotografía

Javier Fuentes



Hace años que he tenido el honor y el privilegio de relacionarme, como consecuencia de la actividad de DINTEL, con militares de carrera de muy alta graduación. Nunca, hasta ahora, con el militar de mayor rango en nuestras Fuerzas Armadas, después de S.M. El Rey. En todos, siempre he encontrado -y ¡disfrutado!- del envidiable control personal que demuestran y la impronta de autoridad innata, que les acompaña como un halo. indisociable con su personalidad.

Pues bien, todas estas virtudes -entre otras más-, caracterizan a nuestro entrevistado, el "General nº 1 de Cuatro Estrellas", General del Aire Excmo. Sr. D. José Julio Rodríguez Fernández, actualmente Jefe de Estado Mayor de la Defensa-JEMAD. Pero, además, José Julio -al que no le importa dejarse llamar así fuera del inevitable

protocolo-, tiene un encanto personal natural que, lejos de restarle un ápice de autoridad, le ensalza y desmitifica. Yo, me imagino así a esos *grandes generales* reconocidos por la Historia, líderes que nunca ordenan pero que arrastran con una mirada.

Conocí, hace ya varios años, al por entonces simplemente General de División, Excmo. Sr. D. José Julio Rodríguez Fernández, cuando era Adjunto al Inspector General CIS del Ministerio de Defensa. Seguí, con sano orgullo de amigo que admiraba su brillante trayectoria profesional, su ascenso a Teniente General y sus iniciativas al frente de la DIGAM en Defensa, como máximo responsable de su Dirección General de Armamento y Material... más de una vez, me encontré con él en la T4 de Barajas a muy primeras horas de la mañana, dirigiéndose a Bruselas para defender los intereses de España.

Como sería prolijo
detenerse enumerando
misiones de su brillante Hoja
de Servicios, coherente con su
ascendente carrera militar, no
me detendré en ello. Lo cierto
es que sólo ha necesitado 39
años exactos para recorrer el
escalafón completo, desde que
saliese de la Academia General
del Aire en julio de 1969 –con

21 años y 1 mes- como
Teniente de Aviación (empezó
pilotando aviones de caza F5
en el Ala 21 con base en Morón
de la Frontera), hasta ser
nombrado JEMAD y ser
promovido a General del Aire,
el 18 de julio de 2008.

El General del Aire José Julio Rodríguez Fernández, está en posesión de las siguientes condecoraciones:

Gran Cruz de la Real y Militar Orden de San Hermeregildo

Gran Cruz del Mérito Aeronáutico

Placa, Encomienda y Cruz de la Real y Militar Orden de San Hermeregildo

Tres cruces del Mérito
Aeronáutico y, entre los
muchos Premios que ha
recibido, destacaré el que yo
más valoro –lógica e
interesadamente-: Premio
DINTEL 2010 "Profesionales
IT" a la "Trayectoria
Profesional". Gracias, José
Julio, mi General, por
aceptarlo, prestigiando con ello
a nuestra Fundación DINTEL.







General, ¿qué es un "General del Aire" en nuestros Ejércitos, y cómo se asciende hasta esta cúpula de la carrera militar?. ¿Cuál es el equivalente con otros Ejércitos, como el de Estados Unidos o la OTAN?

General del Aire es el máximo empleo en el escalafón del Ejército del Aire, es un general en cuyo divisa hay cuatro estrellas; al igual que se hizo en el Ejército de Tierra y la Armada, es un empleo que se creó para dar una mayor relevancia al cargo de Jefe de Estado Mayor de los Ejércitos y la Armada.

También cubría un hueco que existía respecto a países aliados, particularmente de la OTAN, que tenían oficiales generales de cuatro estrellas, mientras España sólo tenía de tres, lo que impedía que militares españoles pudiesen acceder a algunos puestos de la estructura OTAN.

En el marco aliado OTAN, se conoce mediante el acrónimos OF-9 y para todos los países OTAN es un "oficial general de cuatro estrellas", independientemente del nombre que recibe en cada país y dentro de cada país en cada Ejército.

¿Cómo se llega? Se accede a este empleo cuando el Gobierno te designa como Jefe de Estado Mayor de tu ejército respectivo, o de la Defensa como es mi caso. Supongo que en cada caso de los que hemos tenido el honor de acceder a este puesto, ha sido por motivos distintos.

Pero los que hemos alcanzado esta cuarta estrella, tendremos una cosa en común, espíritu de servicio, con lo que ello conlleva. No creo que haya una receta, pero el amor a España y el servicio a su sociedad son obligados.

Se puede decir, sin lugar a dudas, que el Plan Director CIS ha cumplido con creces sus expectativas y sigue siendo un plan vivo y dinámico que evolucionará al ritmo de los avances tecnológicos

Por las responsabilidades que ha desempeñado en su brillante carrera militar, está acreditado que usted tiene un buen conocimiento de la evolución tecnológica de la Defensa de España. ¿Qué papel juegan en ella las Tecnologías de la Información y las Comunicaciones?

De igual modo que las relaciones sociales, económicas y culturales son cada vez más dependientes de las tecnologías e infraestructuras de información y comunicaciones (TIC), éstas se han convertido también en una herramienta vital en el desarrollo de las operaciones en el entorno militar. Consciente de ello, el Ministerio de Defensa está haciendo una importante inversión en la constitución de un Sistema de Mando y Control Militar (SMCM), sustentado en un sistema de información (CIS) que permita proporcionar la información necesaria en el momento oportuno a nuestras Fuerzas Armadas (FF.AA.), desde el entorno táctico al estratégico.

Sin embargo, en el entorno militar no se puede estar al filo de los desarrollos tecnológicos, ya que hay en juego vidas que dependen de la exactitud, oportunidad y veracidad de la información que se maneja. Por ello, se deben utilizar tecnologías suficientemente probadas y consolidadas. Es decir, hemos de estar a la última, pero dentro de un límite de confianza y seguridad en las garantías de la tecnología.

¿Qué punto de desarrollo llegó a alcanzar y hasta dónde se ejecutó el Plan Director CIS del Ministerio de Defensa?

Se puede decir, sin lugar a dudas, que el Plan Director CIS ha cumplido con creces sus expectativas. Está proporcio-

zona + en el diván









nando un excelente servicio tanto de voz como de sistemas informáticos al usuario, en nuestro caso los componentes del Ministerio de Defensa.

En mi opinión, el Plan Director CIS ha sabido anticiparse a las necesidades que supondría el desarrollo exponencial de las denominadas TIC planificando y desarrollando con antelación las soluciones más adecuadas. Se han unificado procedimientos, tanto de contratación como de gestión, se están utilizando los mismos sistemas y herramientas informáticas independientemente del puesto de trabajo, en aras de una mayor interoperabilidad, y se ha logrado una mayor eficacia y eficiencia en el empleo de los recursos económicos y materiales.

Debo añadir que el Plan Director CIS sigue siendo un plan vivo y dinámico que evolucionará al ritmo de los avances tecnológicos. Actualmente se están desarrollando potentes herramientas informáticas en el área del denominado Sistema de Mando y Control Militar

(SMCM). En este sentido, la Subdirección General TIC (heredera de la IGECIS) está colaborando y apoyando la implantación del denominado Sistema de Información Militar. Estos apoyos se materializan en desarrollos concretos de aplicaciones informáticas como pueda ser, entre otras muchas, el Sistema de Mensajería Militar segura (SIMENFAS) o el Sistema de Gestión y Coordinación Logística de Operaciones para las Fuerzas Armadas (SILOGFAS).

¿Qué se entiende, en el Ministerio de Defensa, por Infraestructuras Críticas? ¿Está cambiando el concepto? ¿Por qué?

Como sabe, el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) es la entidad que tiene asignada la responsabilidad de coordinar las actividades de los agentes implicados en la protección de las Infraestructuras Críticas, tanto en el sector público como el privado, para la elaboración de planes generales de protección, así como de planes específicos de sector.

Este Centro trabaja con un gran número de instituciones de la Administración del Estado, entre ellos el Ministerio de Defensa, que lo hace a través de la Dirección General de Infraestructuras (DIGENIN).

En este sentido el Ministerio de Defensa asume la definición del Centro que define a las infraestructuras críticas como "aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".

Más que el concepto, lo que evoluciona, son las infraestructuras críticas que entran en esta definición, el más claro ejemplo son las tecnologías de la información, que en los últimos años han evolucionado de tal manera que han variado completamente los elementos a incluir como infraestructuras críticas.







¿Sería posible, de alguna manera, que se subcontrataran las infraestructuras TIC de Defensa? ¿Por qué?

En Defensa, las infraestructuras TIC se enmarcan en dos entornos, el relativo a Propósito General y el específico de Mando y Control, cada uno con sus propias características y requisitos de seguridad.

El primero, bajo la responsabilidad de la Dirección General de Infraestructura del Ministerio de Defensa, da servicio a las funciones administrativas del Ministerio, mientras que el segundo proporciona los servicios para ejercer el mando, control y seguimiento de las operaciones militares.

En el ámbito de Mando y Control, que es el que está bajo mi responsabilidad, la subcontratación de infraestructuras TIC debe abordarse teniendo en cuenta en primer lugar los requisitos de seguridad y criticidad de los servicios y en segundo lugar el beneficio económico que ésta produciría. Lo principal es garantizar la seguridad de las personas en operaciones y el mando, control y seguimiento de

éstas, por lo que sólo tras un estudio riguroso algunos servicios podrían sub-contratarse. En algunos casos ya se viene haciendo desde hace varios años, tanto a nivel nacional como de la OTAN, como es el caso de la subcontratación de sistemas de respaldo para comunicaciones con las correspondientes medidas de seguridad.

¿De qué forma realizan las FF.AA. españolas la I+D+i en materia de seguridad?

Con carácter general todas las necesidades de las Fuerzas Armadas se integran dentro del Planeamiento de Defensa por Capacidades que se elabora anualmente. Este Plan responde de una forma eficaz y eficiente a las nuevas necesidades de Defensa ante la aparición de las nuevas amenazas, debiéndose buscar a través de I+D+i la respuesta más adecuada.

Una vez decidida la obtención, se inicia el proceso que se estructura en una serie de fases en las que se llevan a cabo el estudio de todos los aspectos relacionados con esta obtención: tecnologías, costes, plazos, interoperabilidad, etc.

Este proceso comienza con la identificación de una carencia o necesidad y un primer estudio de la capacidad que puede dar solución a la misma. Durante las sucesivas fases se va profundizando en el análisis de las posibles soluciones hasta poder determinar la más idónea. Las soluciones que requieren actividades de I+D+i vienen además apoyadas por una serie de iniciativas dentro del Ministerio que tratan de canalizar y facilitar su desarrollo.

Así, la Estrategia de Tecnología e Innovación para la Defensa (ETID) que está siendo desarrollada por la Subdirección General de Tecnología y Centros (SDG TECEN), trata de proponer, promover y gestionar los planes y programas de I+D de sistemas de armas y equipos de interés para la defensa nacional, en coordinación con los organismos nacionales e internacionales competentes en este ámbito.

Esta Estrategia incluye un área de actuación específica en seguridad TI,



disponiendo de un embrión para la experimentación y simulación en seguridad en el Instituto Tecnológico de la Marañosa (ITM).

¿Cómo es la colaboración entre las FF.AA. y la industria TIC?

Podría decir que correcta, adecuada y provechosa, permitiendo que los programas de obtención, que son de responsabilidad del Estado Mayor de la Defensa (EMAD), alcancen un conocimiento real del estado de la tecnología, hagan participe a la industria nacional de las necesidades CIS de las FF.AA., así como de la especificidades de ciertos requisitos del entorno militar para el desarrollo de los productos.

¿Son comparables las tecnologías TIC utilizadas por las Fuerzas Armadas Españolas con las utilizadas por las Fuerzas integradas en la OTAN?

En efecto, las TIC utilizadas por nuestras FF.AA. son comparables a las utilizadas por la OTAN. Prueba de ello es que España ya proporciona servicios de su





sistema conjunto de telecomunicaciones en apoyo a las comunicaciones estratégicas y desplegables de la OTAN. Aunque debo decir que esto no siem-

Aunque debo decir que esto no siempre significa que sean compatibles, debido principalmente a la falta de estandarización existente en muchas líneas de productos. Por ello, nos encontramos en un momento en el que la clave de las TIC es la interoperabilidad, lograda mediante la utilización de estándares definidos por las organizaciones de estandarización. En este sentido, la OTAN, y con ella las naciones de la Alianza, están comprometidas con el objetivo de hacer sus redes interoperables y lograr una federación de sistemas que facilite el desarrollo del concepto de información en red (NEC).

¿En qué medida se utiliza tecnología española dentro de la OTAN?

En lo que se refiere a infraestructuras de telecomunicaciones, la industria española está iniciando su aportación a los nuevos desarrollos que está realizando la OTAN en diferentes campos, tales como la tecnología SCIP (Secure Communications Interoperable Protocol), el sector SATCOM (Satellite Communications), el sector TACOMS (Tactical Communications) o la tecnología SDR (Software Defined Radio).

Además, la aparición del ciberespacio como nueva dimensión está dando nuevas oportunidades dentro de la OTAN a la industria española. El catálogo de productos de seguridad de la información de la OTAN (NATO Information Assurance Product Catalogue) incluye varios productos pertenecientes a empresas españolas, alguno de ellos ya adquiridos.

En general, la necesidad de modernización en los aspectos de telecomunicaciones y cifrado han generado oportunidades para empresas españolas, siendo uno de los campos de trabajo de empresas, tales como 'EPICOM', 'TECNOBIT', 'INDRA', etc.

Como Jefe de Estado Mayor de la Defensa, ¿cuáles considera son sus tres mayores preocupaciones en materia de seguridad? ¿Por qué?

Como se puede imaginar, mi principal preocupación es alcanzar la máxima

capacidad operativa y la seguridad de nuestros militares y personal de apoyo en las diferentes misiones en las que están presentes las FAS. Esto es una preocupación constante y por la que estamos trabajando permanentemente.

La seguridad requiere dotar de medios adecuados a nuestras tropas, tanto en zona de operaciones como en territorio nacional en su apoyo a estas misiones. Pero la seguridad no son solo medios, la seguridad es aptitud y actitud, y éstas no se logran más que con el trabajo diario que realizan los Ejércitos y la Armada en la preparación de su personal.

La importancia de la tecnología en el desarrollo y apoyo a las operaciones, así como la facilidad de acceso a la misma y el aumento de las amenazas asociadas a su uso, hace que la seguridad CIS haya cobrado especial importancia en los últimos años, siendo el ciberespacio la "quinta dimensión" a tener en cuenta.

¿Qué significa la pertenencia a la OTAN desde el punto de vista de la seguridad? ¿Cómo ha cambiado esta visión después de la reunión de Lisboa celebrada los días 19 y 20 del pasado mes de noviembre?

La pertenencia a la OTAN significa un compromiso por una visión común dentro de la Alianza, por los valores democráticos y por los principios de solidaridad, cohesión e indivisibilidad de la seguridad. El propósito fundamental de la OTAN es salvaguardar la libertad y seguridad de todos sus miembros mediante mecanismos políticos y militares, siempre en consonancia con el derecho internacional.

La cumbre de Lisboa ha venido a reforzar está visión de la OTAN por la seguridad, adoptando un nuevo Concepto Estratégico válido para dar respuesta a las nuevas amenazas de la próxima década y así permitir la adecuada defensa a los países miembros frente a éstas. Entre estas amenazas, la relativa al ciberespacio ha adquirido una destacada importancia, por lo que se deben potenciar las capacidades en ciberdefensa en todos los países miembros y la cooperación entre ellos.

La OTAN, y con ella las naciones de la Alianza, están comprometidas con el objetivo de hacer sus redes interoperables y lograr una federación de sistemas que facilite el desarrollo del concepto de información en red



¿Cómo afectan las reducciones presupuestarias a las inversiones en Defensa?

A la hora de establecer los presupuestos siempre hemos tenido en cuenta que nuestra principal preocupación es conjugar la máxima eficacia operativa con la máxima seguridad posible de las tropas desplegadas en el exterior, especialmente en Afganistán y Líbano.

Así, para la mejora de la seguridad de nuestros soldados, nuestra estrategia pasa por un plan de renovación de vehículos blindados, que mejoran la protección balística y antiminas de los vehículos utilizados actualmente; un plan de UAV del ET, que facilitan información e inteligencia de los riesgos en las zonas de despliegue y operaciones; y, un programa de inhibidores, que evitan el accionamiento de dispositivos explosivos accionados a distancia

Afortunadamente las reducciones que ya se habían iniciado anteriormen-

te no afectan a los programas principales de adquisición, tales como el 'Leopardo', las fragatas 'F-100', el 'Eurofighter' y otros. Además, los programas de adquisición de material siguen sus plazos.

Entre otras medidas, para optimizar los recursos disponibles, lo que se está haciendo es racionalizar los contratos de externalización, centralizar y priorizar al máximo posible de adquisiciones o utilizar medios de enseñanza a distancia y online, así como el empleo intensivo de simuladores.

¿Podría mejorarse la utilización del presupuesto de Defensa? ¿Por qué?

La respuesta está implícita en la contestación anterior, el Ministerio de Defensa y las Fuerzas Armadas hacen un importante esfuerzo para continuar con sus planes, a pesar de la reducción de los presupuestos. Hay un elemento no

negociable que es la seguridad de nuestras tropas en el exterior y a partir de ahí se establecen unas prioridades y se racionaliza el gasto.

¿Cuáles son las misiones más onerosas que lleva a cabo el Ejército Español? ¿Sería posible dejar de realizar alguna de ellas? ¿Por qué?

En primer lugar, tengo el orgullo de afirmar que nuestras FF.AA. son más operativas y están mejor equipadas que nunca y su rendimiento en Zona de Operaciones es excelente.

Sin embargo, no se puede cuantificar el esfuerzo desarrollado por los militares españoles en cada una de las misiones en las que España participa y, por tanto, establecer una clasificación al respecto. Cada misión tiene sus particularidades, con sus ventajas e inconvenientes, hablando desde un punto de vista operacional.



Las operaciones militares en el exterior suponen un compromiso adquirido con la sociedad española, tras el consenso adoptado en el Congreso, como parte de nuestra política exterior. Y, como muestra de ese compromiso, permanecemos sobre el terreno hasta que cumplimos los objetivos marcados, tal y como ha ocurrido recientemente con Bosnia, tras casi 20 años de presencia, y, como ocurrirá en Afganistán, al transferir gradualmente las responsabilidades a las autoridades afganas.

¿Sobre qué tema no le hemos preguntado que le gustaría añadirnos sus comentarios?

Consciente de que la importancia que tiene esta nueva "quinta dimensión", no podría dejar pasar esta oportunidad para hablar de la importancia que tiene para nosotros, dentro del ámbito militar, la ciberdefensa.

Así, el EMAD organiza anualmente jornadas técnicas y, cada dos años, con-

ferencias de concienciación sobre seguridad de la información. Por su parte, el Centro Superior de Estudios de la Defensa Nacional organiza, también con carácter anual, unas jornadas de seguridad de la información del Ministerio para concienciar y sensibilizar al personal civil y militar en esta materia.

Es más, desde hace dos años, España participa activamente en diversos grupos de trabajo, simposios y ejercicios internacionales sobre ciberdefensa, siendo en 2009 cuando organizó el primer ejercicio de ciberdefensa de las FF.AA., lo que nos permitió conocer las capacidades técnicas existentes en materia de ciberdefensa en el Ministerio, así como una primera aproximación de los diferentes centros y unidades con recursos humanos y conocimiento en esta área.

En el marco de la OTAN, España fue uno de los siete países europeos que pusieron en marcha en 2008 el Centro de Excelencia de Cooperación en Ciberdefensa (CCD COE) de Tallin (Estonia). Actualmente, militares españoles trabajan en el departamento de doctrina y adiestramiento y en el departamento de investigación y desarrollo.

Asimismo, España participa en la cumbre de directores de seguridad de la información CIS de países de la OTAN y en el subcomité de seguridad de la información de la OTAN, donde se tratan a alto nivel el estado, retos y problemas de la seguridad de los sistemas CIS de la OTAN y, en especial, la problemática relacionada con los de mando y control desplegados en operaciones.

Por lo que respecta a la Unión Europea, España trabaja desde 2009 en el Estado Mayor de la Unión Europea para la definición del concepto de 'operaciones de ordenadores en red' en el marco de operaciones militares lideradas por la Unión Europea.