LA PLATAFORMA DIGITAL DE LA *F-110*

Luis Francisco ASTORGA GONZÁLEZ

AS nuevas construcciones de la Armada se enfrentan a un futuro tecnológico que se puede denominar como disruptivo: los vehículos autónomos y la inteligencia artificial (IA) cambiarán durante el siglo XXI de forma radical la manera de combatir y la concepción de las operaciones navales. Es difícil predecir cuándo va a suceder, pero que va a pasar casi ningún analista lo duda.

La Armada necesita reemplazar las fragatas clase *Santa María*, que están en el último tercio de su vida operativa. El nuevo programa de fragatas *F-110*, ya definido y que entrará en servicio a partir de la mitad de la próxima década, llega, en cierta medida, un poco demasiado pronto y un poco demasiado tarde. Pronto porque hoy en día no se dispone ni de la experiencia ni de la tecnología adecuadas para incorporar, de forma extensiva, las capacidades de IA y los vehículos autónomos a los que hemos hecho referencia; y tarde, porque la obsolescencia de las capacidades de las *F-80* hace que estos buques no puedan ya operar con solvencia en el agitado panorama internacional, en el que parece que los escenarios de baja intensidad están dejando paso a los de alta complejidad, muy exigentes en prestaciones para buques polivalentes tipo fragata.

Para esa nueva fragata *F-110*, en la que es muy improbable que vayamos a disponer, cuando entre en servicio, de inteligencia artificial, al menos de forma extensiva, sí que es una certeza que va a incorporar mucha más conectividad y automatización que la que tienen las plataformas actuales. Conectividad y automatización que, si bien proporcionarán nuevas capacidades, también requieren novedosas formas de operación y exigen por lo tanto la transformación de la organización.

La plataforma digital de la *F-110* y de los buques sucesivos llevará múltiples redes de ordenadores alámbricas e inalámbricas, enlaces vía satélite, servidores de datos, de comunicaciones, electrónica de red, etc. ¿De qué características? No importa. Todo esto son «tornillos». No tiene ninguna importancia si por ejemplo se instalan servidores HP y electrónica de CISCO o si el *hardware* es de IBM y HUAWEI. En la *F-110* —nuestros buques del futuro— lo que nos debe preocupar son los condicionantes que determinarán el diseño de sus sistemas informáticos, el personal con el que los vamos a operar y sostener, cuánto y qué se va a externalizar y cómo y con qué conectaremos sus sistemas.

Para saber a dónde vamos, es a veces necesario echar la vista atrás y ver cuál ha sido el camino recorrido, con sus luces y sus sombras. Como decía Ortega y Gasset, «el tigre de hoy y el de hace 10.000 años son iguales, pero los hombres de hoy y los de hace doscientos años no somos iguales, porque el peso de la historia condiciona nuestra manera de ver el mundo». Eso es lo que le ocurre a la Armada, que en cierta medida se comporta como un ser vivo: aprendemos de nuestro pasado y lo proyectamos al futuro. Y quizá en el tema CIS/TIC (1) necesitemos una reflexión serena sobre dónde estamos y cómo hemos llegado hasta aquí para poder dotarnos de las estructuras que la organización necesita para operar con éxito los sistemas del siglo XXI.

Evolución de los sistemas de la Armada

Es importante recordar que los buques de guerra (y en particular los submarinos) están probablemente entre los ingenios más complejos que ha construido el hombre, porque a veces se nos olvida, incluso a los miembros de la Armada. Una fragata es un conjunto de sensores y sistemas de armas, capaces de operar por debajo y por encima del agua e incluso hasta el espacio ultraterrestre, ubicados en una plataforma marítima resiliente, con capacidad de desplazarse a altas velocidades y sostenerse y albergar a su dotación durante meses lejos de su base. Ello dentro de las obligadas limitaciones de espacio que impone el compromiso entre supervivencia al combate, capacidades, precio, etcétera.

Una complejidad en cierto sentido integrada pero «silente»: los miles de equipos instalados a bordo de una fragata *DEG*, buques construidos en Ferrol en los años setenta del pasado siglo, tenían que encajar en el espacio

(1) *Communication and Information Services*/Tecnologías de la Información y Comunicaciones. En este artículo usaremos indistintamente ambas denominaciones, que corresponden al mismo concepto: CIS se usa en el mundo militar y TIC en el civil.

disponible y coordinarse en peso, tamaño, ubicación, estabilidad, redundancia y un largo etcétera; pero en general, y salvo por el contacto que produce la ubicación física, los distintos elementos se ignoraban unos a otros, no se comunicaban. Y si lo hacían era a través de señales eléctricas analógicas dentro de sistemas específicos, de un modo que consideraríamos hoy muy primitivo.

El grupo de combate (el *Príncipe de Asturias* y las fragatas *F-80*) y los primeros diseños modernos de Bazán, la actual Navantia, cambiaron un poco esta situación en los años noventa, primero con los sistemas de combate de las *F-80* y su integración para el combate «multi-buque» a través de redes tácticas, como Link 11, y luego en el seno de los propios buques, de forma interna, con los desarrollos de los sistemas de control integrado de plataforma (SICP) concebidos por Navantia.

A los sistemas de combate, que integran las armas y sensores de una unidad con los de la Fuerza, y a los de control de plataforma, que conectan y automatizan los elementos de energía propulsión y servicios, se añadieron también, desde mediados de los años 90, las comunicaciones de datos vía satélite. Desde entonces estos sistemas no han dejado de crecer en la Armada. Inicialmente conectaban a los buques con los estados mayores en tierra por vía telefónica o a través de sistemas rudimentarios de mando y control (C2), que fueron mejorando a gran velocidad. De comunicaciones tácticas a nivel local —básicamente en el alcance visual con los otros buques de la fuerza— se pasó a disponer de enlaces con el mando en tierra y sistemas de mando y control y logísticos en red hasta el nivel operacional. Para ello se usó fundamentalmente la red de área extensa del Ministerio de Defensa, una herramienta puesta en marcha en su día por la extinta Inspección General CIS (IGECIS) y que ha incrementado la conectividad y productividad del Ministerio de una forma asombrosa. Sobre esta red se han montado muchísimos servicios, incluidos algunos de comunicaciones —como el correo electrónico corporativo—, pero priman las aplicaciones de gestión: repuestos, mantenimiento, personal, contabilidad, pagos, etc., que han mejorado notablemente los procesos de trabajo y la eficiencia de la organización.

Así que, *grosso modo*, tenemos, o teníamos, a principios de siglo XXI tres dominios relativamente diferenciados: sistemas de combate, sistemas de control de plataforma y las aplicaciones montadas en la red de área extensa de MINISDEF (WAN PG), fundamentalmente para servicios logísticos.

En la figura 1 se describe la situación de la conectividad de las plataformas navales en el año 2000. En verde, los enlaces tácticos de datos (TDL), conectados con otros buques de la fuerza en redes *ad hoc* a nivel local (con los de su Task Group), y por otro lado, las redes de ordenadores de a bordo, conectadas a redes de área extensa: a la red corporativa del MINISDEF. A estas hay que añadirles algunas otras clasificadas OTAN, como la NSWAN, que en el tramo

nacional se conecta a través de la red de transporte (WAN IPC2) del Sistema Conjunto de Telecomunicaciones Militares, SCTM, separada de la WAN PG.

Salvo por algunas estaciones de trabajo de las redes OTAN clasificadas y las comunicaciones tradicionales radio de la Armada (gestionadas a través de un sistema informático específico, SACOMAR), con carácter general podemos decir que en las últimas décadas la Armada ha funcionado con estos entornos separados de comunicaciones y sistemas.

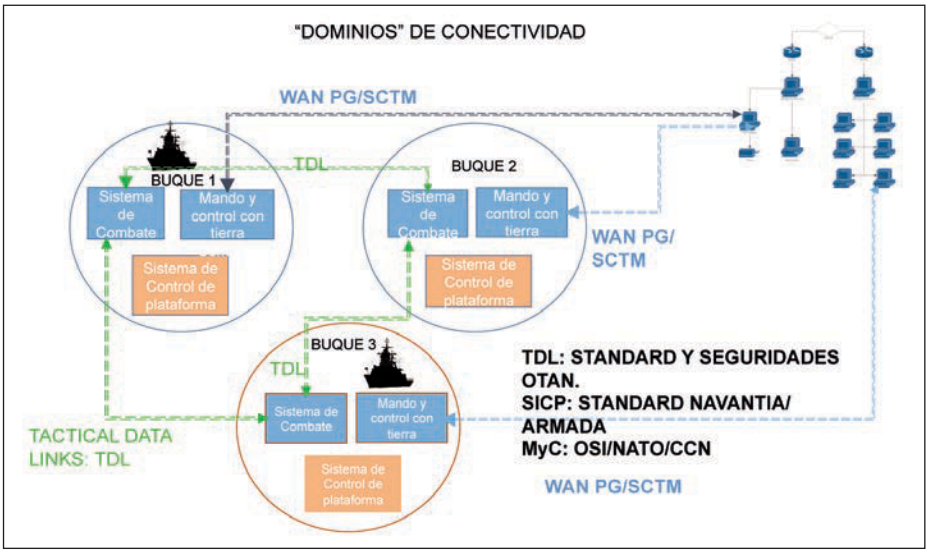

Figura 1.

El pandemónium de estándares y seguridades

¿Con qué estándares y seguridades se trabaja en estos dominios? Para sistemas de combate, por los fijados por la OTAN, en realidad por Estados Unidos, que ha sido y sigue siendo nuestro principal proveedor. Se incluyen aquí los sistemas de cifra y claves para interconectar plataformas. Para los sistemas de control de plataforma se utilizan los fijados por Navantia, que son básicamente industriales. Para la logística con tierra —a través de la WAN PG, que es una red no clasificada—, tenemos estándares industriales con seguridades corporativas. Y finalmente, para los sistemas y redes clasificadas de C2 (que operan en la WAN IPC2), se aplica la normativa fijada por la Organización Nacional de Seguridad (ONS), adscrita al CNI, cuyas funciones son asegurar la protección de la información clasificada. Es importante resaltar: las funciones de la ONS son asegurar la protección de la infor-

mación clasificada (2). La falta de doctrina y normativa nacional de seguridad sobre sistemas ha hecho que se esté empezando a aplicar «a todo» la normativa de la ONS, que lógicamente responde a la cultura de la organización en la que está embebida: el CNI, un centro que orienta toda su actividad a la obtención y análisis de inteligencia. Su activo principal es la información, que hay que proteger a toda costa. Para las FF. AA., esta no es un fin, sino un medio que debe preservarse hasta el momento en que las medidas de protección no impidan o lesionen de manera grave el cumplimiento de las misiones operativas de las unidades.

El problema de la aplicación de la normativa de la ONS es fácil de comprender cuando se ve cuál es la evolución de la interconexión de los sistemas que describíamos en la figura 1 hasta una situación que es potencialmente como la actual, descrita en la figura 2, donde describimos un único buque —una sola de las tres burbujas que representábamos en la figura 1— en el que interconectamos: a) el sistema de combate, los sistemas de mando y control y la plataforma entre sí; y b) todos estos sistemas con sus correspondientes en tierra. ¿Por

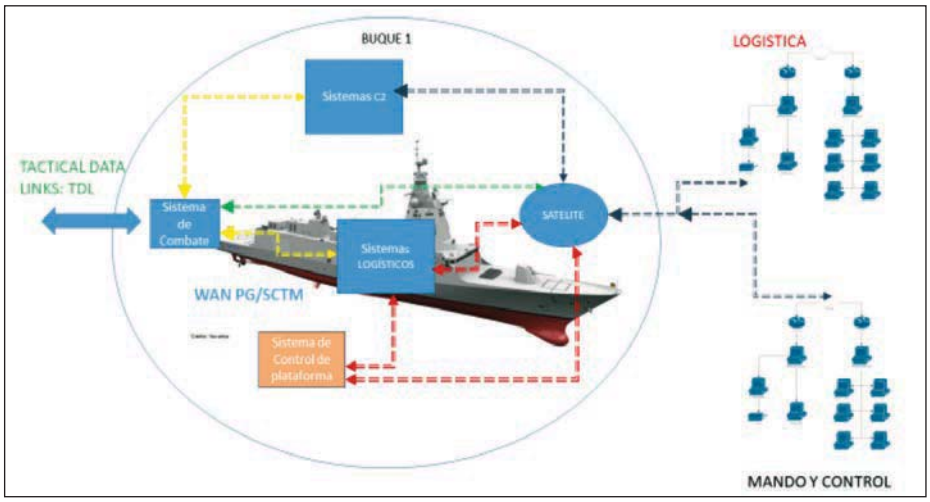

Figura 2.

(2) La normativa básica emitida por la ONS comprende las normas siguientes:

— NS/01: Estructura nacional de protección de la información clasificada.
— NS/02: Seguridad en el personal. Habilitación personal de seguridad.
— NS/03: Seguridad física.
— NS/04: Seguridad de la información.
— NS/05: Seguridad de los sistemas de información y comunicaciones.
— NS/06. Seguridad industrial.

qué es necesario hacer esto? Podemos ilustrarlo con algunos ejemplos. Los planes de vuelo de aviación civil, en los que se dispone de la identificación y los códigos 3 de IFF de los aviones comerciales, se presentan en las consolas de guerra aérea del sistema de combate para ayudar al operador a elaborar la situación aérea, RAP. También porque puede que haya que compartir la situación táctica con un buque que esté a cien millas náuticas; para ello, y puesto que se está fuera del alcance UHF, se necesita empaquetar la información de Link 16 por NIRIS, sistema que corre en la NSWAN y que permite el intercambio de trazas en tiempo útil a través de la red. Otro caso podría ser el de la extracción de los datos de funcionamiento de elementos de la planta propulsora, como las turbinas de gas, que se reciben en el sistema de control de plataforma y se transmiten a través de la red logística para su análisis en tierra y poder así pasar de un mantenimiento correctivo a uno predictivo (3).

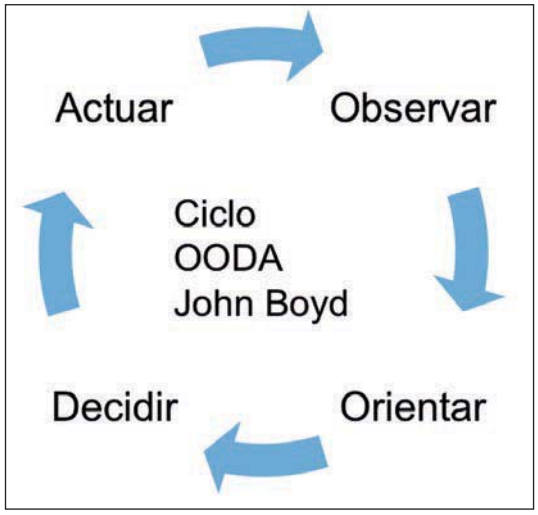

Figura 3.

Hay quien piensa que estas interconexiones no son necesarias, que presentan riesgos de seguridad y que por ejemplo no hace falta que la información IFF recibida de aviación civil se muestre de forma automática en las consolas tácticas. Pero si el *Vincennes* la hubiera tenido, nunca habría derribado al *A300* iraní que despegaba de Bandar Abbas (4).

Cada vez se dispone de más información que procede de múltiples fuentes (y de multitud de redes), que indefectiblemente tiene que procesarse e inyectarse a los sistemas C2 de forma automática si se quiere disponer de un ciclo OODA (5) (*Observe-Orient-Decide-Act*) más rápido que el del adversario. Esta es la esencia del concepto NEC (*Network Engagement Capability*), incorporado a la doctrina de las FF. AA. desde hace ya más de un decenio.

(3) Esa es la función del CESADAR.

(4) En 1988 un avión comercial de Iran Air, con 255 pasajeros a bordo, que viajaba de Teherán a Dubái, fue derribado por un misil SM-2 del USS *Vincennes* al confundirlo con aviones de caza.

(5) Creado por el coronel John Boyd, del US Air Force.

¿Cuál es el problema de las interconexiones de redes? Pues que requiere acreditar de forma específica cada interconexión y sus pasarelas, de forma que se asegure que no pasa información desde redes de clasificación superior a otras de clasificación inferior, independientemente de clasificación de la información que se intercambie. No se puede conectar el sistema de combate de una *F-100* a través de NIRIS con otra fragata o destructor sin acreditar todos los nodos intermedios y las pasarelas entre redes siguiendo la normativa de la ONS, la cual no está pensada para estos sistemas.

Se puede razonar que lo que hay que hacer es acreditar los sistemas/redes y las pasarelas que sean necesarias. Lamentablemente esto no es viable. Su número crecerá exponencialmente en el futuro. Y es, con la normativa actual, un proceso muy complejo que requiere de demasiados recursos.

Ilustremos el problema: para un ejercicio OTAN de defensa contra misiles balísticos en el que participó una fragata *F-100*, la acreditación de los nodos, que implicaba a la Armada, al Ejército del Aire y al CESTIC, llevó varios meses, estuvo a punto de no conseguirse —se contó con cierta benevolencia de la ONS— y el buque estuvo a punto de no participar en un ejercicio en el que se habían empleado muchos recursos, al que había costado mucho acceder y en el que se probó una capacidad estratégica que puede ser esencial para la seguridad nacional: que las FF. AA. dispongan en el futuro de medios efectivos de defensa de zona contra misiles balísticos.

Necesitamos una política de seguridad para nuestros sistemas y esa política no puede ser la de la protección de la información tal y como hoy en día está concebida. Como se ha señalado, la información es un medio para llegar a un fin. La posición de un equipo de operaciones especiales en el terreno es sin duda información clasificada —aunque de validez temporal muy corta—, pero si es necesario comunicarla por radio en claro para proporcionar apoyo aéreo urgente porque no hay otro medio de transmitir la información, se hace; el cumplimiento de la misión y la seguridad del personal van antes que la protección de la información.

La doctrina clásica definía cuatro principios para las comunicaciones militares: confianza, seguridad, rapidez y flexibilidad, incompatibles entre sí, ya que disponer, por ejemplo, de mucha rapidez y flexibilidad se hace a costa de disminuir la fiabilidad y la seguridad. Las soluciones perfectas no existen y es necesario adoptar compromisos que posibiliten el cumplimiento de la misión, que es la que determina cómo se diseñan las comunicaciones y no al revés.

La reciente arquitectura global de telecomunicaciones de MINISDEF elaborada por el CESTIC establece un marco de referencia para el diseño y explotación de los servicios de comunicaciones; básicamente intenta racionalizar la estructura definiendo los servicios por capas horizontales, de forma que todo lo que necesite cada uno para funcionar que no esté en su capa o nivel se solicite (o proporcione) a las capas inferiores (superiores). Esto tiene ventajas y desventajas. La orientación al cliente de esta estructura por capas

limita el número de interfaces y aplicaciones, ahorra costes en licencias y simplifica mantenimiento y soporte, pero también tiene inconvenientes, porque es difícil alcanzar la fiabilidad del funcionamiento de las aplicaciones verticales, que no se ven afectadas por las evoluciones de las diferentes capas de la arquitectura, casi nunca en sincronía.

La dificultad de implementar una arquitectura horizontal por servicios es inmensa dentro de la WAN PG; en todo caso, esta arquitectura no soluciona el problema de seguridad que presenta la hiperconectividad. Y desde mi humilde punto de vista, es el reto operacional y el problema técnico más grave y de mayor impacto al que se van a enfrentar las FF. AA. —no solo las españolas— en la próxima década.

Los buques del futuro

En la *F-110* o en una hipotética futurible *F-120* dispondremos de una maqueta digital —un reflejo virtual del buque real— que facilitará la gestión logística bajo los estándares de la Industria 4.0, con el propósito de incrementar la disponibilidad operativa a un menor coste y mejorar el adiestramiento de la dotación. Realidad aumentada, realidad virtual, Internet de las Cosas (IoT) son herramientas que ya están disponibles y que se irán incorporando a los nuevos buques. Habrá que hacerlo con prudencia, sin dejarse arrastrar por las modas tecnológicas; la utilidad de algunas aplicaciones, que suponen mucho coste de adquisición y de mantenimiento, debe ponderarse con un cuidado análisis de coste/eficiencia.

La explosión de la sociedad de la información y de las tecnologías asociadas hará que los buques futuros lleven a bordo de miles de elementos con capacidad para conectarse e interactuar digitalmente con su entorno; no solo el inmediato, también el lejano. Entre otras razones porque es lo que habrá en el mercado: el IoT (Internet de las cosas) es imparable.

Los siguientes son algunos ejemplos sencillos de servicios ya funcionando o que lo harán a muy corto plazo: sabremos con precisión qué repuestos tenemos a bordo, de manera que cuando se instale uno en un equipo se generará una petición automática para su reemplazo. También podremos saber dónde está cada miembro de la dotación y cuáles son sus constantes vitales, acceder al manual actualizado o al plan de mantenimiento de un equipo en una PDA o en unas gafas de realidad virtual sin necesidad de buscarlo navegando por un árbol infinito de documentación. Recibiremos una alerta desde tierra que nos dirá que el generador número dos se va a romper y que debemos pararlo y arrancar y meter en carga el número tres.

El buque dispondrá de una COP que se formará con sensores propios y remotos y enlazará en redes tácticas de forma inteligente con sus UAV y USV o con los de otras unidades terrestres, navales o aéreas de forma automática o

semiautomática. Se intercambiarán vídeo, audio, señal radar, cartografía, información meteorológica, AIS, de vuelo, etc., de forma dinámica y a demanda según la situación táctica. Un tercero disparará nuestras armas con sus datos o viceversa.

Podemos intentar poner coto a ese flujo de información y control, pero resultará imposible. Ese torrente de datos va a ser imprescindible no solo para disponer de una COP que acelere el ciclo OODA, sino también para poder operar las futuras plataformas navales, que van a incorporar equipos que en su gran mayoría seguirán estándares tecnológicos civiles y por ello se verán obligados a seguir procedimientos de actualización, mantenimiento, etc., similares a los equipos vendidos en el sector civil, lo que exigirá conectividad a internet.

La promesa del *Network Engagement Capability* de proporcionar en el campo de batalla el intercambio de datos «inteligente» entre los planos de información, sensores y armas a múltiples plataformas— y cuya implementación no ha sido hasta la fecha posible más que de forma parcial— empieza ya a estar al alcance de la frontera tecnológica, especialmente con el uso de inteligencia artificial. Esa conectividad, que se establecerá a nivel táctico y operacional, no va a poder funcionar aislada del resto «del mundo» por las razones que antes apuntamos. Intentar mantener entornos estancos es como negarse a abrir las compuertas de la presa en caso de crecida; retrasará la inundación, pero cuando se produzca, porque finalmente se abran las puertas o la presa reviente, las consecuencias serán mucho peores.

Como todo en la vida, el progreso trae ventajas e inconvenientes. Hoy es ya técnicamente posible en algunos buques actuar sobre la propulsión, arrancar y parar un generador eléctrico o abrir una válvula del circuito de contraincendios desde tierra vía satélite. Y por tanto es también teóricamente posible hackear esos sistemas y hacer que actúen de forma errática o maliciosa. La solución al problema no es negarse a esa conectividad, sino adoptar estrategias a largo plazo para poder aprovechar las ventajas de las nuevas tecnologías reduciendo los riesgos asociados. El objetivo debe ser mitigar —que no resolver, porque es imposible— el problema, que inevitablemente acabará afectando también a los sistemas de armas. Estas estrategias deben partir de tres premisas básicas:

— La hiperconectividad no se puede evitar.
— La seguridad perfecta no existe —sigue la ley de los rendimientos decrecientes, por lo que la seguridad 100 por 100 tiene un coste infinito.
— El análisis y gestión de riesgos de conectividad debe pasar a formar parte del corazón de la cultura de la organización.

Ni el entorno operativo de los próximos treinta años ni los procedimientos de trabajo de las unidades navales van a responder a decisiones de la Armada.

En el primer caso porque ni el progreso tecnológico ni la evolución del escenario internacional son variables sobre las que tengamos influencia; únicamente podemos intentar anticiparnos haciendo prospectiva, algo nada sencillo. Y en el segundo porque vamos a seguir operando en alianzas, y el peso de los Estados Unidos en los procedimientos operativos domina a todos los demás actores. Si no hay un vuelco muy improbable en el escenario internacional, en los próximos decenios seguiremos siendo aliados de los Estados Unidos y usando una gran cantidad de procedimientos OTAN en las operaciones conjunto-combinadas.

Es por tanto necesario que la Armada haga un prudente ejercicio de prospectiva y se prepare para actuar en aquellos elementos sobre los que sí podemos decidir: el personal y la organización.

Personal y estructura CIS/TIC

El personal y la orgánica CIS/TIC de la Armada han sufrido muchas modificaciones en los últimos decenios; también lo ha hecho la filosofía de trabajo.

Haciendo de nuevo un poco de historia, en la Armada la informática comenzó con el empuje que le dio el Cuerpo de Intendencia y que se plasmó en la adquisición de grandes ordenadores (HOST/MAINFRAMES) de IBM para aplicaciones de personal, nómina y repuestos. El campo se amplió pronto a los sistemas de combate de las corbetas clase *Descubierta* y del Grupo Aeronaval; esto hizo que se organizaran cursos en el extranjero y luego se crearan especialidades específicas —analista y programador— para así disponer de personal técnico capacitado para soportar y mantener las aplicaciones de gestión y los programas operativos de las fragatas clase *Santa María* y del *Príncipe de Asturias*.

La Armada en la década de los noventa del pasado siglo tenía varias docenas de analistas y más de un centenar de programadores desarrollando y haciendo mantenimiento de aplicaciones. Este personal se ubicaba repartido entre el CPT/CÍA, el CPT de Cartagena, el CPD central y los CPD periféricos. Nada se parece aquel escenario a la situación actual: no se dispone de ningún analista y hay solamente uno o dos programadores en toda la Armada que actúen como tales. Hemos pasado de desarrollar y mantener aplicaciones, en muchos casos exclusivamente con personal de la Armada, a la situación actual, en la que nos circunscribimos a administrar ordenadores y redes, e incluso para esto necesitamos ayuda externa. Cuando nos hace falta una aplicación, por simple que sea, se la contratamos a un tercero.

La estructura de la Jefatura CIS, que incluye a la mayoría del personal en apoyo en tierra que realiza labores CIS, dispone de unas 700 personas en plantilla. No es una cantidad pequeña para una Armada de veinte mil; a ellas hay que añadirle el personal CIS de los buques y unidades de IM: en números

redondos, podemos hablar de unos 1.000 individuos, el 5 por 100 del total del personal de la Armada, dedicados a labores CIS. Nuestro modelo CIS requiere mucho personal por razones estructurales, algunas consustanciales a la naturaleza de la Armada (número elevado de buques) y otras difíciles de modificar a corto plazo: una elevada dispersión geográfica, disponer de siete estaciones radio, de un Centro de Comunicaciones principal en Madrid (CECOMMAD) y su alternativo en Rota y de gran número de personal dedicado en exclusiva a comunicaciones por radio (6). No obstante, incluso con los condicionantes estructurales señalados, el número de personal CIS es alto y hay que admitir que su rendimiento, con carácter general, es escaso. Ello es sobre todo por falta de competencia técnica en algunas áreas, especialmente en las de programación y administración de sistemas. Las razones de la baja cualificación profesional son fundamentalmente dos: escasa permanencia en los destinos y falta de reciclaje. La formación que se proporciona en las escuelas no es mala —aunque, como todo en la vida, es mejorable—, pero no se retiene al personal en destinos CIS/TIC una vez ha cumplido sus condiciones tras acabar la especialidad.

La única forma de acumular capital humano CIS es fomentar su permanencia en los destinos y generar una dinámica de continua actualización de conocimientos. Hay diversas alternativas para lograrlo: cambios en el reglamento para forzar la permanencia, mejora de la valoración profesional de los destinos, proporcionar complementos económicos, reducir o suprimir las condiciones de embarque… Lo que resulta palmario es que la política actual de la Armada con el personal CIS lo que hace es desincentivar su permanencia, con lo que la descapitalización de conocimientos CIS a la que hemos llegado en los últimos años es muy preocupante. Desgraciadamente las nuevas unidades no nos van a exigir menos en términos de gestión CIS, sino mucho más: es por ello necesario revisar con urgencia la política de personal de los oficiales y suboficiales CIS/TIC, para asegurar que tengan una formación adecuada, que permanezcan en los destinos sin menoscabo de su progresión en el escalafón y que permanezcan en un continuo reciclaje formativo.

También la estructura CIS de la Armada ha experimentado cambios importantes en los últimos 25 años. Hemos tenido División CIS en el EMA, Centros de Procesos de Datos, Centros de Comunicaciones, que luego se mezclaron con los de procesos para crear los CIGAS; y finalmente ahora disponemos de una Jefatura CIS de la que depende un grupo de centros de explotación CIS en el que se juntan orgánicamente las estaciones radio y los antiguos CIGAS, que han sido rebautizados como CECIS (7). Ya no existe la División CIS, y la plani-

(6) De las 700 personas de JECIS, 250 están asignadas a las estaciones radio, que se operan en remoto desde CECOMMAD.

(7) Centro de Explotación CIS.

ficación de los sistemas y la política CIS es responsabilidad de las Divisiones de Planes, de Logística y de la estructura conjunta (el EMAD o el CESTIC).

Es cierto que la DIVCIS nunca resultó demasiado útil. No se consiguió articular con continuidad una política específica para los sistemas de información —sí para los de comunicaciones radio— y la División se dedicó sobre todo a la gestión y control de los sistemas existentes o planificados por la estructura conjunta. Tampoco de todos: fueron con el tiempo proliferando sistemas que se han quedado al margen de la DIVCIS/Jefatura CIS, como el portal de procesos, las aplicaciones de gestión de personal y algunas de gestión económica o de mantenimiento, lo que ha contribuido a incrementar el desconcierto sobre lo CIS en la organización.

Las nuevas construcciones exigen que la Armada se dote de una política CIS específica y que la haga la JECIS o una de las divisiones del EMA. No todo lo que se determina en el CESTIC es aplicable a la Armada, por la especial idiosincrasia de los buques, y la complejidad CIS de las unidades que se avecinan nos exigen adaptar la organización si no queremos fracasar estrepitosamente. Por poner un ejemplo, el control de configuración *software* y la política de actualización del *firmware* de las decenas de miles de equipos que llevarán las nuevas construcciones será un reto mayúsculo incluso si se dispone de la estructura adecuada. De no ser así no habrá control de configuración y algunos equipos dejarán de funcionar, debido a actualizaciones de *software* no compatibles entre sí y sin que quizá seamos capaces de revertir fácilmente la situación.

Una estructura en la que tendremos que determinar qué áreas deberemos externalizar y hasta qué punto habrá que hacerlo. No compensa económicamente hacer todo con personal de la Armada: algunas funciones tendremos que conservarlas por razones de seguridad o porque son de importancia capital; pero como antes señalábamos para las *suites* tecnológicas, para delimitar qué externalizamos habrá que hacer igualmente un detallado análisis de coste/beneficio.

Conclusiones y propuestas de futuro

El concepto NEC, alumbrado conceptualmente hace casi dos décadas, se ha desarrollado hasta la fecha de forma limitada debido a condicionantes tecnológicos, pero todo apunta a que las tecnologías de la revolución 4.0 propiciarán en el próximo decenio un cambio disruptivo en la explotación de ese concepto. No cambiará la naturaleza de la guerra, pero obligará a transformaciones revolucionarias en el empleo de los medios en los niveles táctico y operacional. El progreso de las tecnologías de la información, del IoT, de la inteligencia artificial y en general de la hiperconectividad que incorporarán nuestras plataformas navales, comenzando por la *F-110*, nos obligan a acome-

ter, a medio plazo, una transformación muy importante en la Armada para poder operar y sostener esas unidades futuras con éxito.

La necesidad de algunos cambios es evidente: ni la estructura, ni la política de personal, ni de seguridad CIS/TIC pueden continuar como hasta la fecha. De hecho ya se ha empezado esa transformación, con iniciativas como los planes PROA o CORAL, que abordan algunos de los problemas que se han planteado en este artículo.

Se mencionó antes la necesidad de hacer prospectiva y a partir de ahí definir la transformación que requerirá la Armada. Una prospectiva —junto con un diagnóstico de la situación actual— que solos no seremos capaces de hacer adecuadamente. Tenemos agujeros en nuestro *know how* que nos exigirán apoyarnos en consultoría externa y en organismos ajenos a la Armada, como por ejemplo el Centro Conjunto de Desarrollo de Conceptos y el CESTIC.

La Armada siempre ha sido capaz de adaptarse a las transformaciones tecnológicas y del entorno para operar y mantener con éxito sus buques. No hay duda de que también lo hará con las fragatas *F-110* y con las unidades que lleguen en el futuro, llevando a cabo las modificaciones orgánicas y los cambios en la formación y carrera del personal CIS que sean necesarios. El reto es continuar siendo una Marina de Guerra de primer nivel, capaz de afrontar con solvencia los enormes desafíos que nos esperan a lo largo de este turbulento siglo XXI.