NO PERDER EL NORTE: UN AÑO ENTRE EL BÁLTICO Y LOS FIORDOS NORUEGOS

Luis DE MEDINA REDONDO

... pues lo que resulta con toda claridad del horrible ejemplo de la guerra pasada es que nuestra escuadra estaba organizada y vivía en el supuesto de que no había de tener más adversarios que combatir que carlistas, tagalos o marroquíes. Cuando se ha encontrado con una marina moderna, pertrechada y municionada, ha sucumbido con demostraciones de heroísmo admirable y de resignación sublime para el martirio en tripulaciones y jefes, pero sin lograr eficacia militar alguna.

Francisco Silvela

Cambio de escenario: del mediodía mediterráneo al sol de medianoche

EN mi último año en el empleo de capitán de corbeta tuve la oportunidad de pasar destinado al Estado Mayor de la SNMG-1, donde estuve al frente de la sección N-6, entre otros cometidos. Así, a primeros de julio de 2018 salí de España y llegué a Dinamarca para embarcar en el buque insignia de la agrupación. Y eso supuso un cambio mucho mayor que el mero viaje en avión, porque el escenario en el norte es muy distinto al que nos tiene acostumbrados el Mediterráneo y también más allá de Suez.

Esto tiene una cierta lógica. Tras el fin de la Guerra Fría, la Alianza Atlántica se encontró sin un rival militar digno de ese nombre con la desaparición del Pacto de Varsovia. La superioridad tecnológica de las fuerzas occidentales era incontestada en las distintas intervenciones militares llevadas a cabo, desde la Operación TORMENTA DEL DESIERTO hasta la UNIFIED PROTECTOR. En el entorno marítimo, nos acostumbramos a ver en los grupos de combate de portaviones (CVBG) unas herramientas multipropósito capaces de desplazarse a cual-

quier teatro de operaciones y proyectar el poder aeronaval sobre distintos oponentes que poco o nada podían hacer para resistirse.

Además, con objeto de incrementar la eficacia y la eficiencia de las acciones tácticas, se pasa a implementar conceptos tipo *net-centric*, como el *Network Centric Warfare* estadounidense, iniciativas encaminadas a aprovechar los principios y las tecnologías de la era de la información para el desarrollo de operaciones militares. Y eso conlleva una enorme dependencia de sistemas CIS, cuya vulnerabilidad no preocupaba porque no se tenía en frente a un rival tecnológicamente avanzado.

Más aún, desde los comienzos del presente siglo nos hemos ido poco a poco habituando a operaciones de lucha contra el terrorismo, como ACTIVE ENDEAVOUR, SEA GUARDIAN o la más lejana LIBERTAD DURADERA, o contra la piratería, como OCEAN SHIELD o ATALANTA, e incluso orientadas al reto de la migración ilegal, como SOPHIA. Por tanto, nuestra experiencia institucional en las dos últimas décadas se ha escorado más hacia el ámbito de la seguridad marítima, a escenarios de baja intensidad.

Sin embargo, no son el único tipo de escenario en el que podemos vernos involucrados en base a nuestros compromisos internacionales. En 2014, Occidente se topó de bruces con una realidad diferente, encontrándose que la posibilidad de enfrentarse a rivales globales o regionales con capacidad tecno-

Agrupación SNMG-1. (Foto: *www.flickr.com/photos/armadamde*).

lógica suficiente para suponer un serio desafío (*near pear rivals*) ya no era algo impensable (1). Además, son rivales que han ido tomando nota de los puntos fuertes y débiles que caracterizan a las fuerzas armadas occidentales, orientado en base a ello sus desarrollos tecnológicos y doctrinales. La combinación de estos avances técnicos con una actualización de la doctrina sobre defensa en profundidad es lo que nos lleva al A2/AD (*Anti-Access/Area Denial*), del que el Báltico es uno de los ejemplos más claros, como pude apreciar durante los meses en que la SNMG-1 operó en él.

De los estrechos daneses al golfo de Finlandia: la burbuja A2/AD del Báltico

El A2/AD podría considerarse como las capacidades militares solapadas a través de múltiples dominios con la intención de infringir el mayor nivel de atrición posible en las fuerzas adversarias. El objetivo es simple: generar zonas o burbujas «seguras» a las que el enemigo no pueda acceder ni siquiera con sus armas convencionales de largo alcance o, en el caso de que sea capaz de desplegarse en ellas, se vea incapaz de operar eficazmente.

La componente A2 es la que trata de impedir la llegada al teatro de operaciones mediante el empleo de medios de largo alcance que son capaces de atacar al oponente mucho antes de que este sea capaz de hacer lo propio. Así, las fuerzas navales y aéreas que pretendan acceder al teatro de operaciones experimentarían un nivel de atrición tan elevado que o bien no estarían en condiciones de operar o bien optarían por no acercarse y, por tanto, ceder la victoria.

Eso es lo que buscan sistemas de armas como los misiles antibuque hipersónicos (2) y los balísticos (3) antibuque, principalmente. Su teórica capacidad es superar las defensas de los CVBG e infringir serios daños a los portaviones mucho antes de que objetivos rusos en el Báltico queden dentro del alcance de los aviones lanzados por estos. Además, estos aviones también se encontrarían con la amenaza de potentes sistemas antiaéreos, lo que añade una

---

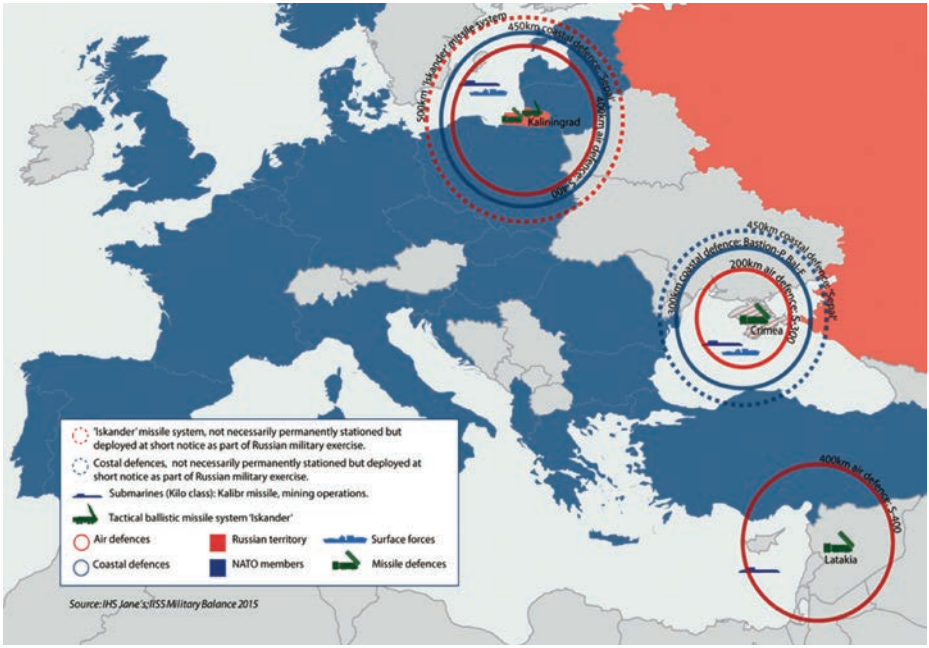
(1) Aunque este artículo se centra en las capacidades rusas, son también especialmente significativos los casos de China, Corea del Norte o Irán, por citar solo unos ejemplos.

(2) Ese es el caso del SS-N-33 Zircon, del que la información disponible en diversas fuentes proporciona cifras de un alcance de 250 millas y una velocidad terminal Mach 6, que superaría la capacidad de interceptación de misiles como el Sea Ceptor *(https://nationalinterest.org/blog/buzz/royal-navy-cant-stop-russias-hypersonic-3m22-zircon-missile-97972)*.

(3) Por ejemplo, el sistema Bastión-P de misiles supersónicos de 150 millas de alcance y cuya presencia en Kaliningrado contribuye al A2 por la estrechez de los accesos al Báltico desde el oeste (RIPLEY, TIM: «Moscow's missions: Russian expeditionary warfare capabilities». *Jane's Defence Weekly*, 22/01/2019).

capa AAW extra al A2 ruso (4) del Báltico con estos sistemas desplegados en el enclave de Kaliningrado.

La componente AD se refiere a las acciones encaminadas a impedir las operaciones de nuestras fuerzas en áreas en las que el adversario no puede o no va a impedir nuestro acceso. El AD, por tanto, afecta a la capacidad de maniobra dentro del teatro de operaciones contra la que actúan medios de menor alcance. En el caso del Báltico, no solo sería la capacidad ofensiva de los buques rusos, que incluso en tiempo de paz hacen un constante *shadowing* de las fuerzas navales aliadas que operan allí, sino también la de los cazabombarderos que realizan frecuentemente pasadas sobre esas fuerzas. Y ello sin olvidar las baterías lanzamisiles costeras móviles que, llegado el caso, serían una amenaza para grandes buques (portaviones, anfibios, logísticos y mercantes), afectando tanto a la libertad de maniobra en el Báltico como a la seguridad de las comunicaciones marítimas.



Descripción parcial de capacidades A2/AD en el Báltico, mar Negro y Mediterráneo Oriental. (Fuente: *IHS Jane's; IISS Military Balance 2015*).

(4) Según informaciones disponibles en fuentes abiertas, el S-400 sería capaz de enfrentar blancos aéreos a casi 200 millas siempre que volasen por debajo de 100.000 pies de altitud *(https://elpais.com/internacional/2019/07/12/actualidad/1562946364_806211.html)*.

Y aquí habría que añadir la parte submarina. Centrándonos en el caso ruso; es significativa la entrada en servicio de diez submarinos en la última década (para sus cuatro flotas, no solo del Báltico) y los planes de repetir esa cifra para el próximo lustro. Son unidades que están equipadas con torpedos de supercavitación (5) o misiles antibuque de nueva generación (6), ante los que los portaviones se mostrarían extremadamente vulnerables.

Y este ejemplo del Báltico de burbuja A2/AD «marítima» no es único en el mundo, sino que podemos encontrar otros, como alrededor de la península de Kola, en el mar Negro apoyándose en Crimea o en el Mediterráneo Oriental, ahora con la base de Tartus disponible para fuerzas rusas. Y si no nos limitamos al caso ruso, también las vemos en grandes áreas del Pacífico (China y Corea del Norte) o en los accesos al golfo Pérsico (Irán). Así, son numerosas esas burbujas frente a las que el poder ofensivo de los CVBG se ve, como mínimo, muy limitado.

Del mar del Norte al Báltico: contrarrestado el A2/AD

La respuesta occidental ante ese nuevo concepto de A2/AD parece estar articulándose en dos líneas de trabajo diferentes, pero no excluyentes entre sí. La primera consiste en incrementar el esfuerzo en desarrollos tecnológicos con la intención de que nos permitan extender el alcance ofensivo de los sistemas de armas al menos hasta una distancia igual a la que uno de los posibles rivales es capaz de hacerlo.

Por otro lado, dado que esos desarrollos requieren tiempo, la otra línea de trabajo es la generación de nuevos conceptos doctrinales que buscan minimizar la efectividad de las burbujas A2/AD. Así, tenemos el caso significativo de la Marina estadounidense que traslada el concepto de operaciones distribuidas al ámbito marítimo, desembocando hace pocos años en lo que se ha denominado Letalidad Distribuida (7).

En base a esta nueva orientación táctica, en lugar de potentes CVBG, que resultan muy vulnerables, serían empleados varios grupos de un número relativamente pequeño de escoltas (SAG), entre cinco y siete, de gran potencia de combate, como buques *Aegis* o equivalentes. Siguiendo distintas derrotas, sin ofrecer ningún blanco de importancia tan crítica como un portaviones y cuya

---

(5) Como el VA-111 Shkval, del que algunas fuentes estiman su velocidad en 200 nudos *(https://nationalinterest.org/blog/buzz/meet-russias-shkval-supercavitating-torpedoes-us-has-nothing-them-80241)*.

(6) Ese es el caso del Kalibr, del que hay variantes tanto de ataque a tierra como antibuque (WILLETT, Lee: *Sub-Surface Competition in the Euro-Atlantic Area*, Éditoriaux de l´Ifri, Ifri, 2 octubre 2019).

(7) ROWDEN, Thomas; GUMATAOTAO, Peter; FANTA, Peter. *Distributed Lethality*. US Naval Institute. *Proceedings*, enero 2015.

neutralización, por tanto, tendría un efecto mucho menor, dificultarían el *targeting* del oponente y reducirían la efectividad de la componente A2.

Luego, una vez en el teatro de operaciones, la existencia de varias SAG permite que estas puedan desplegarse por él, operar con distintos niveles de discreción y minimizar la eficacia del *targeting* del rival, así como compartir la información obtenida por sus sensores sobre una región más amplia, en base a una moderna arquitectura CIS. Esta tendría un efecto multiplicador, haciendo que las acciones fueran más eficaces y eficientes a nivel táctico y operacional, con capacidades tales como *Cooperative Engagement Capability*, el JREAP, etcétera. En resumen, también se produce una reducción importante de la efectividad del AD.

Se hace aquí necesario resaltar que la viabilidad de este desarrollo doctrinal, que guarda similitudes con el actual concepto de *Standing Naval Forces* (SNF), se basa en la disponibilidad de una arquitectura CIS robusta y potente, lo que también es una vulnerabilidad. En otras palabras, los sistemas CIS que la soportan son un nuevo punto crítico contra el que se dirigiría la acción del adversario, que buscará así atacar nuestra capacidad de mando y control.

Navegando por el mar de Noruega y el Báltico: C2D2E

Durante la fase de ejecución del ejercicio TRIDENT JUNCTURE 2018, los gobiernos suecos y finlandés informaron de perturbaciones en los sistemas GPS en distintas áreas a un lado y otro de la península escandinava y cuyo origen atribuyeron a Rusia. Este caso constituye un ejemplo muy significativo, ya que la pérdida de señal GPS sería una de las maneras con las que un oponente buscaría generar entornos donde la capacidad de mando y control sea degradada o negada (*Command and Control Degraded or Denied Environment*, C2D2E).

La generación de C2D2E se consigue mediante acciones en distintos campos, incluso dominios, encaminadas a negar o degradar los sistemas satelitales, tanto de comunicaciones como de GPS, y también las comunicaciones radio. Los desarrollos tecnológicos de las últimas décadas también han ofrecido una amplia variedad de vectores que pueden ser explotados para llevarnos al C2D2E.

La degradación o anulación de los sistemas satelitales puede ser obtenida por ataques físicos (acciones *hard-kill*) mediante el empleo de armas ASAT, que van desde misiles antisatélite (8) hasta propios satélites que provoquen

(8) Hace algo más de 10 años, China demostró que, además de Rusia y Estados Unidos, también tenía esa capacidad (*https://www.nytimes.com/2007/01/18/world/asia/18cndchina.html*).

colisiones, sin descartar en un futuro próximo el uso de armas de energía dirigida. También es posible mediante perturbación, como la mencionada unos párrafos antes, o detonaciones nucleares en las capas altas de la atmósfera que generen pulsos electromagnéticos.

Las consecuencias de que se vean degradados o anulados nuestros sistemas satélites afectarían a los sistemas de mando y control que se apoyan en enlaces SATCOM, enlace del que somos cada vez más y más dependientes y cuya resistencia a acciones hostiles no ha recibido suficiente atención.

En el caso del GPS, la pérdida de su señal afecta negativamente a sistemas PNT (*Positioning, Navigation and Timing*). Así, se puede llegar a anular la efectividad de armas con guía GPS, provocar pérdidas o errores en la presentación de sistemas de combate, negar comunicaciones fiables y seguras (9) o generar errores en la navegación cuyas consecuencias variarán en función de las condiciones ambientales.

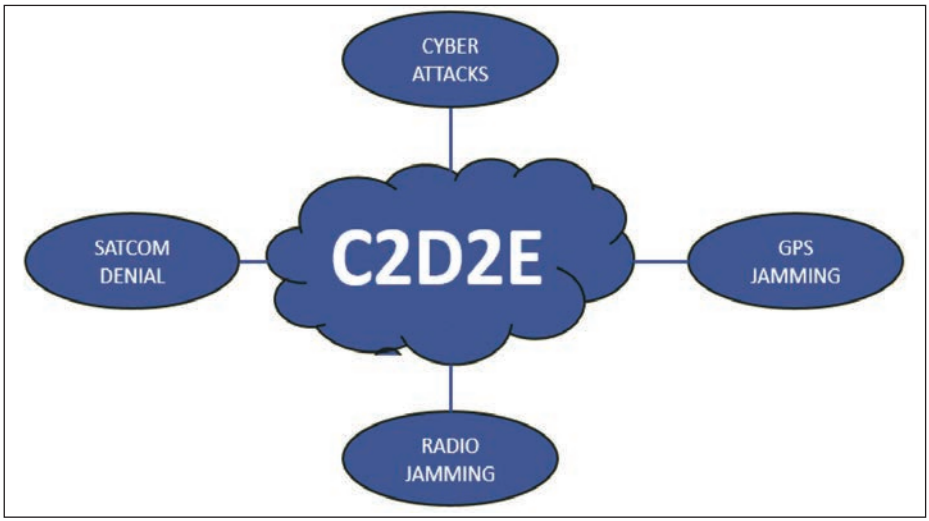
En lo concerniente a las comunicaciones radio, la presencia de sistemas de altas prestaciones (10), tanto en el enclave de Kaliningrado como en la zona del Múrmansk, se traduce en la generación de zonas donde es posible la perturbación del espectro radioeléctrico, pero también el análisis de señales radio que lleven a la identificación y localización de la fuente o la obtención de información. Incluso en la situación actual, el empleo de estos sistemas puede orientarse a la generación de un entorno en el que los operadores sean incapaces de distinguir si la degradación en el medio radioeléctrico es intencionada o no. Es decir, que no sea fácil distinguir si estamos ante una degradación por causas ambientales, una interferencia o una perturbación que, en todo caso, impide operar con normalidad.

Y además de acciones en los ámbitos satelital y radioeléctrico, también algunas de las realizadas en el dominio del ciberespacio pueden ser empleadas en la generación de C2D2E. Los ciberataques, dentro de sus múltiples posibilidades, pueden estar dirigidos contra los equipos AIS, estaciones de anclaje de sistemas satélite, los propios satélites, equipos radios del tipo *Software Defined Radio* (SDR) o los sistemas C2, por citar solo algunos de sus posibles objetivos.

---

(9) La señal de tiempo proporcionada por el GPS da una referencia de tiempo utilizada por equipos radio de salto de frecuencia (como el *Have-Quick II*) para la sincronización de los saltos. También es usada por determinados equipos criptográficos para sincronizar tiempos para la cifra empleada.

(10) Por citar un solo ejemplo, el Borisoglebsk-2 ha sido especialmente diseñado para actuar contra enlaces de comunicaciones, tanto radio como SATCOM, así como sistemas de navegación satélite.



Entre Gotland y Kaliningrado: contrarrestando el C2D2E

La forma de contrarrestar la generación de C2D2E sigue un patrón similar a lo indicado para el A2/AD, esto es, mediante innovaciones técnicas y tácticas. Entre las primeras, encontramos diversos proyectos en diferentes estados de desarrollo destinados a dar robustez a la arquitectura CIS de las agrupaciones navales, muchos de ellos ya conocidos por la Armada; algunos están orientados a los sistemas SATCOM (empleo de frecuencias EHF, implementación de ECM, por citar solo algunos), mientras que otros a sistemas radio —MARLIN (11), *Wide Band HF*, BRIPES (12), SATURN (13) o CHESS (14), entre otros—.

En el ámbito táctico, hay también otras líneas de trabajo enfocadas a mejorar la seguridad de las comunicaciones en agrupaciones navales mediante una

(11) Acrónimo que identifica al sistema *MARitime Line of sight Network*, capaz de soportar un sistemas C2 mediante enlaces radio de UHF.

(12) *BRASS IP Enhacement System*, innovación en cuya primera Arquitectura Técnica conocida como BRE1TA (*BRASS Enhancement One Technical Architecture*) ya trabaja la Armada.

(13) SATURN, *Second Anti-jamming Tactical UHF Radio for NATO*, que reemplazará a un ya veterano *Have Quick II*.

(14) *Correlated HF Enhance Spread Spectrum*. Estándar de salto de frecuencia en HF para la OTAN, que puede ser usado en combinación con otros sistemas, como BRE1TA o el próximo TDL LINK 22.

reorientación del adiestramiento. De la experiencia obtenida en estos meses como miembro del Estado Mayor de SNMG-1, en algunos casos se trata de novedades, mientras que en otros encontramos la aplicación de métodos y procedimientos ya conocidos pero poco practicados, incluso desaparecidos en algunas de las marinas aliadas. Estas actuaciones pueden ser organizadas en tres grandes categorías, en función de si están orientadas a sistemas satélite, a comunicaciones radio o al ciberespacio.

Dentro de lo concerniente a satélites, la mayoría de los casos están encaminados a reducir la dependencia que se tiene de ellos y mejorar la capacidad para operar en entornos donde el uso de SATCOM es negado (*SATCOM denial)*. Actualmente, por ejemplo, la mayoría de los ejercicios OTAN comienzan a incluir períodos de duración variable en los que se simulan escenarios de *SATCOM denial*, a menudo de manera repetida y cada vez más largos, superando fácilmente las 24 horas. En esas «ventanas» se dejan de utilizar servicios C2 que son soportados por los enlaces SATCOM, tales como el *JChat*, y se maximiza el uso de comunicaciones radio, tanto para voz como para datos (mensajería ACP-127).

A mitad de camino entre el ámbito de satélites y el de enlaces radio, se está trabajando en el adiestramiento *Counter Surveillance Satellite* (CSS), orientado a aquellos casos en los que el oponente usa satélites para localizar las agrupaciones navales en base a sus emisiones UHF, SHF y EHF. Estas frecuencias no experimentan reflexión en la atmósfera y la atraviesan, permitiendo que satélites del rival puedan detectarlas y así triangular para determinar la situación y derrota de nuestras SAG. Conociéndolas, sus acciones para generar C2D2E e incluso para A2/AD serán más eficaces. El adiestramiento en CSS se orienta al empleo de enlaces HF (radiodifusión, buque-tierra y red operativa administrativa de la SAG) y comunicaciones visuales, de forma que se minimiza o anulan las indiscreciones por el uso de comunicaciones radio en UHF o SATCOM.

El empleo de enlaces HF, por otra parte, también resulta indiscreto dentro de la troposfera y son por tanto susceptibles de interceptar para su análisis, perturbación o la localización de la fuente. Por ese motivo, la reducción de la firma HF es objeto de otro de los esfuerzos en adiestramiento, mediante el uso de *broadcast ship-guard* que canalice todo el tráfico de mensajería desde o hacia la fuerza, empleando una red en UHF para la tramitación de mensajes dentro de la SAG.

También es de reseñar el adiestramiento orientado a dar robustez a los circuitos de voz para hacerles más resistentes a la perturbación. El uso de *Have Quick II* (HQ-II) va más allá del mero establecimiento de los enlaces y se busca su utilización de manera habitual para las redes de guerra principal ASUW o AAW. En realidad, se trata de volver a algo que ya se hacía en la Armada hace años, pero que tiene poco uso en escenarios de baja intensidad.

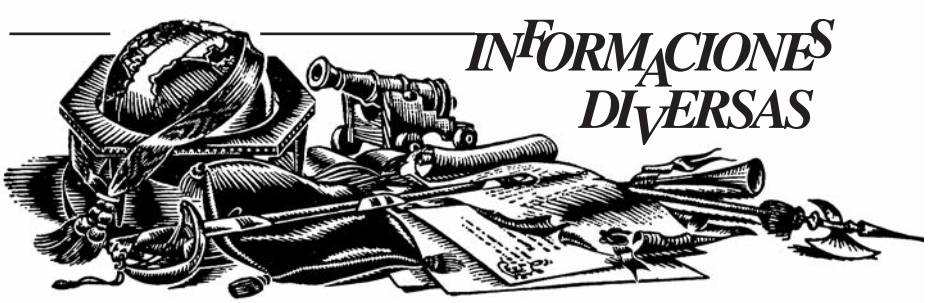
La tercera categoría, relativa al ciberespacio, es más novedosa. Reforzar la ciberdefensa de unidades navales es uno de los objetivos del OPTASK Cyberspace promulgado por MARCOM en noviembre de 2018. En él se fijan las posturas de ciberdefensa en base al nivel de amenaza y las acciones que deben ser ejecutadas acorde a cada una de las posturas. Además, la incorporación de adiestramiento en ciberdefensa como parte de los ejercicios o en el calendario interno de la propia SNMG-1 constituyen una forma eficiente de incrementar tanto el nivel de preparación como el de concienciación de las dotaciones.

Por ejemplo, en JOINT WARRIOR 19-1 las unidades participantes fueron objeto de una campaña de *phishing* de creciente intensidad a lo largo de la duración del ejercicio, de forma que se valoró el nivel de preparación y la rapidez y eficacia de las reacciones. A su vez, para el plan de adiestramiento interno de SNMG-1, la labor coordinada entre la sección N-6 de ese Estado Mayor y la de HQ MARCOM llevaron al diseño y ejecución de distintos adiestramientos en el primer semestre de 2019, bautizados como CYBEREX. Estos tenían una duración variable, normalmente no superior a 24 horas, cubriendo diferentes aspectos de ciberdefensa.

De Noruega a España: reflexiones finales

Desde una perspectiva estrictamente racional, la existencia de escenarios muy diferentes a aquellos en los que estamos habituados a operar no es algo completamente desconocido para la Armada. Conceptualmente, todos sabemos que son posibles. Sin embargo, al igual que les ha ocurrido a otras marinas de países aliados, la experiencia y los cometidos principales de los últimos lustros ha ido llevando a que gran parte de la preparación se oriente a los de baja intensidad, que nos son más inmediatos, tanto en términos geográficos como de intereses nacionales. Y así, los piratas en el océano Índico y en el golfo de Guinea o las mafias de migración ilegal en el Mediterráneo se han ido convirtiendo en la versión actual de los « carlistas, tagalos o marroquíes» del siglo XIX de la cita de Francisco Silvela.

Y aunque sea más frecuente y probable el encuentro con piratas o mafias, no podemos asumir que nunca nos encontraremos en escenarios más demandantes, con burbujas A2/AD reforzadas con C2D2E, el equivalente a esa «marina moderna, pertrechada y municionada» de la cita inicial del artículo. Por tanto, es necesario estar preparados para ello, con el correspondiente esfuerzo tanto en lo que se refiere a la adquisición de sistemas y capacidades como en lo concerniente al adiestramiento.

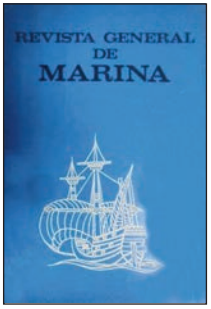


HACE CIEN AÑOS

El número de marzo de 1920 comienza con el artículo titulado *La solución del problema de la subsistencia del personal de la Armada,* del capitán de corbeta Pedro M.ª Cardona. Continúa con: *El armamento de nuestros buques en construcción*, del comandante de Artillería José María Vázquez; *La instrucción y especialización del personal de Máquinas*, del maquinista oficial de segunda Juan B. Méndez, y *Desarrollo de los motores de combustión interna*; en las *Notas profesionales*, encontramos las correspondientes a Alemania, Estonia, Francia, Inglaterra, Japón y Portugal.

Finaliza este número con *Miscelánea, Bibliografía* y *Sumario de revistas.*

HACE CINCUENTA AÑOS



El número de marzo de 1970 comienza con el artículo titulado *Más sobre la fe (Catilinaria)*, del capitán de navío M. Sánchez Alonso. Continúa con *Mi escuela en su XXV Aniversario,* del coronel auditor de la Armada A. Landín Carrasco, y *Situación actual del mundo comunista*, del capitán de fragata Von Wichmann de Miguel.

Entre los dedicados a *Temas profesionales* destacamos: *La rentabilidad de las Fuerzas Armadas*, por el capitán de fragata Senac Calderón; *Aplicación de la energía termonuclear*, del capitán de corbeta ingeniero Sánchez Valdés; *El mar Menor y la jurisdicción en materia criminal*, del capitán auditor de la Armada J. L. Meseguer, y *Un río negro bajo el Atlántico*, de S. D'Artenay.

Continúa este número con *Nota internacional* con el título *Mil días de resistencia*, cuyo autor es el capitán de corbeta J. L. T.; *Miscelánea* e *Informaciones diversas* con el artículo *VIII Salón Náutico Internacional de Barcelona*, de M. Ramírez Gabarrús.

Finaliza este número con *Noticiario* y *Libros y revistas.*

Francisco ORDÓÑEZ MUÑOZ

(Retirado)