APORTACIÓN DE UNA FUERZA NAVAL A LA LUCHA C-IED

Marcos R. DE SOUSA FUCHS

Antonio J. PALMERO ROMERO

Introducción

pesar de la existencia de doctrina OTAN de nivel conjunto respecto a la lucha contra los IED (C-IED) (1), lo cierto es que existe una cierta carencia en cuanto a su implantación en el dominio marítimo aliado. Ello puede ser debido a alguno de los siguientes motivos, entre los cuales podría también darse cierta relación causa-efecto:

— La doctrina C-IED OTAN, si bien «conjunta» y por tanto aplicable en el entorno marítimo, está excesivamente, como el mismo AJP (2) reconoce, orientada al entorno terrestre. Pero también, al mismo tiempo, se da un desconocimiento generalizado por parte de las fuerzas navales de ese enfoque integral y global C-IED.

— La falta de conocimiento de la amenaza que emplean los IED (3) llega a producir una total desvinculación de la fuerza naval con este oponente, sobre todo cuando aquel efectúa sus ataques exclusivamente

(1) Que responde a su acepción anglosajona *Countering Improvised Explosives Devices* (C-IED), es decir, lucha contra los artefactos explosivos de circunstancias o improvisados (IED). Ambas acepciones «de circunstancias o improvisados» son ampliamente utilizadas; no obstante y según el Concepto Conjunto español CCJ-01 «Acciones contra Artefactos Explosivos de Circunstancias (C-IED)» (enero 2010), la primera de ellas es la más correcta.

(2) AJP-3.15(B) *Countering Improvised Explosives Devices*.

(3) Se define el sistema IED como el conjunto de personal, materiales y actividades y las relaciones entre ellos, necesario para concebir, planear y ejecutar un ataque IED y aprovechar sus efectos. El sistema IED comprende al propio IED, al adversario y sus actividades y elementos del entorno geográfico, social y cultural (CCJ-01).

en la dimensión terrestre (4). Y ello, a pesar de que tanto los ataques como las actividades para llevarlos a cabo también se desarrollan en los denominados espacios comunes (5).

— La tradicional postura defensiva de la fuerza naval para hacer frente a las amenazas asimétricas está muy centrada en la reacción contra una amenaza concreta o un ataque en curso, y poco orientada a la estrategia integral o a la ejecución de acciones preventivas.

No obstante, dentro de la OTAN se están dando los primeros pasos para desarrollar una doctrina C-IED naval, lo cual demostraría que se ha detectado su necesidad, y al mismo tiempo solventaría la problemática ya reseñada de falta de mayor implicación de las fuerzas navales en la lucha C-IED. Y hablamos de implicación porque es evidente que la concienciación/mentalización ante este tipo de ataques con WBIED (6) y otras amenazas de carácter asimétrico es, dentro de la Armada, considerable, como de hecho demuestra la implantación en los buques de unas robustas medidas y procedimientos de Protección de la Fuerza (MFP) (7) para hacer frente a la amenaza asimétrica en general y, por tanto, a este tipo de ataques con WBIED (8).

Es quizás también dicha concienciación y la confianza en las medidas de MFP tomadas las que reafirman el convencimiento de aquellos que piensan

---

(4) Aunque la problemática también pudiera ser la falta de adhesión a la acción conjunta, en este caso por todos los servicios del ámbito conjunto. De hecho, no son pocos dentro del mundo naval los que se preguntan qué tiene que ver una fuerza naval en la lucha C-IED.

(5) Los espacios comunes, en su acepción inglesa *Global Commons*, entendidos como los dominios globales, internacionales y supranacionales en donde se encuentran los recursos de la población. Los espacios marítimos internacionales estarían contenidos dentro de esta definición.

(6) En su acepción inglesa, *Water Borne IED*. A pesar de no existir una definición concreta en el ámbito OTAN, habitualmente se refiere a toda variedad de IED que se utilizan en el agua, bien sea en superficie o bajo ella, como por ejemplo embarcaciones y dispositivos submarinos cargados de explosivos, de carácter suicida o activados por control remoto, IED dejados a la deriva flotando o anclados al fondo marino, etcétera.

(7) Al tratarse del concepto de Protección de la Fuerza en el entorno marítimo, se utiliza su sigla inglesa *MFP* que corresponde al término *Maritime Force Proteccion*.

(8) Aunque no tan numerosos como en el entorno terrestre, se puede encontrar un buen número de incidentes marítimos con IED. A nivel nacional, dos buques de la Armada, el destructor *Marqués de la Ensenada* y el patrullero *Tabarca*, ya sufrieron sendos ataques en los años 1981 y 1982 respectivamente. En el plano internacional se pueden encontrar ejemplos muy recientes, como los ataques a los destructores USS *Cole* y USS *Sullivan* en el año 2000, al TVR del USS *Firebolt* en el año 2004 con un IED suicida, los diversos incidentes IED en aguas próximas a la franja de Gaza en los años 2002, 2009 y 2010, los tres ataques con IED suicidas en aguas próximas a Sri Lanka, los ataques a los petroleros *Limburg, Takasuzu* y *M-Star* en los años 2002, 2004 y 2010 respectivamente, o el incidente IED ocurrido en aguas de Libia en 2011. (CDR ALVARADO, Ray: *Countering IED in the maritime domain*. NATO unclassified).

que el componente marítimo tiene poco que decir en C-IED. De hecho esta corriente de pensamiento no es extraña, pues ya se dio en su día en el entorno terrestre, donde el concepto C-IED se ha desarrollado e implantado con mayor rapidez por motivos obvios. Sin embargo, esta estrategia basada exclusivamente en las medidas de protección de la fuerza está hoy en día superada ante la evidencia de que, enfrentado exclusivamente al IED, la amenaza no se minimiza ni se solventa. Y eso es lo que plantea, tanto la doctrina OTAN como la doctrina nacional en C-IED. El concepto C-IED incide actualmente en la necesidad de adoptar una postura eminentemente activa y ofensiva para derrotar al Sistema IED, ganando la iniciativa y por tanto restringiendo el espacio de maniobra del oponente.

WBIED Libia. (Fuente: *www.nato.int*).

La lucha C-IED

La lucha C-IED, tal y como refleja la diversa doctrina ya señalada, no se centra en el propio artefacto, sino que realiza una aproximación integral y global a toda la amenaza, pues no hay que olvidar que el adversario real no es el IED propiamente dicho, sino aquellos que los usan, construyen, transportan, financian, etc. El C-IED necesita del esfuerzo colectivo en todos los niveles de planeamiento (tanto militar como político) y de conducción de las operaciones para conseguir la derrota del Sistema IED. Las operaciones C-IED no deben planearse ni ejecutarse aisladamente, deben ser parte integral de toda la campaña.

Por otra parte, el C-IED tiene un carácter eminentemente «conjunto», al igual que la gran mayoría de operaciones que se llevan actualmente a cabo, en las que la actuación aislada de un solo ejército/armada es impensable. La aportación de cada contingente —Tierra, Mar y Aire— al C-IED no es una cuestión de «suma de esfuerzos», sino que debe entenderse como un «esfuer-

zo común» que produce una sinergia mayor a la realmente derivada de su simple unión.

Las actividades C-IED se engloban en tres líneas de acción o pilares:

— Ataque a las redes IED (AtN) (9), el cual se dirige contra las estructuras del adversario antes de que pueda realizar un ataque con un IED y tiene un marcado carácter activo.
— Anulación de los IED (DtD) (10), que tiene como finalidad evitar el empleo eficaz de un IED una vez que el adversario lo ha emplazado o preparado para su utilización. Este pilar tiene un marcado carácter defensivo.
— Preparación de la Fuerza (PtF) (11) para que las unidades que participen en operaciones donde exista amenaza IED estén instruidas y adiestradas para combatirla.

Los tres pilares están soportados de manera transversal por la necesaria inteligencia y conocimiento del entorno con respecto a la amenaza IED (12) y a su interacción con la población y el entorno físico, actividad que se conoce como «conocimiento e inteligencia» (U&I) (13).

La dimensión marítima en la lucha C-IED

Como ya se ha mencionado anteriormente, es normal que los Sistemas IED puedan actuar en y desde la mar allá donde tengan posibilidades dentro de su zona de actuación. Es decir, que tanto las fuerzas navales como el Sistema IED comparten un mismo espacio de maniobra y, debido al carácter de esta amenaza, normalmente será el entorno litoral. Esto deriva en dos premisas claras: la primera de ellas es que las fuerzas navales (14) pueden llegar a

---

(9) En su acrónimo inglés y que corresponde a *Attack the Network*.

(10) Ídem, *Defeat the Device*.

(11) Ídem, *Prepare the Force*.

(12) Sus características, estructura, organización, puntos críticos de las redes IED, las características en sí mismas de los artefactos usados, etcétera.

(13) También se puede encontrar la denominación «entendimiento e inteligencia». La forma de alcanzar este conocimiento se materializa a través de la función de Inteligencia, y dentro del planeamiento OTAN conforme a la *Comprehensive Operations Planning Directive* (COPD) mediante la correcta preparación integral del entorno operacional (CPOE), específicamente orientado a la evaluación de la amenaza IED o el conocido IPB *(Intelligence Preparation of the Battlefield)* a nivel táctico, igualmente centrado en la amenaza IED.

(14) Nótese que no se habla Fuerzas de Desembarco (proyección del poder naval sobre tierra) por parecer evidente que estas, operando en un entorno terrestre, serían igualmente blanco de los ataques con IED y, seguramente, con mayor probabilidad.

convertirse en un objetivo de los Sistemas IED presentes en el Área de Operaciones Conjuntas (JOA), y la segunda es que todas las actividades de las fuerzas navales influyen, aun no habiendo sido planeadas de forma integral bajo una estrategia C-IED, en todas las actividades y componentes del Sistema IED.

Las fuerzas navales, gracias a las capacidades de que disponen, están desarrollando actualmente algunas actividades que se podrían encuadrar dentro de las líneas de acción de la estrategia C-IED, especialmente en lo relativo a la «Anulación de los IED», y en gran parte a la «Instrucción, adiestramiento y lecciones aprendidas» (15). Pero lo hacen de manera autónoma, sin integrarse en la estrategia global C-IED y como simple respuesta a la posibilidad de sufrir un ataque asimétrico.

Sin embargo, el elemento clave dentro de la estrategia C-IED es la lucha contra las redes IED (AtN), precisamente el pilar más desconocido y donde menos actúan las fuerzas navales. Este pilar se basa en una postura activa, de carácter ofensivo, que ataca directamente la raíz del problema, es decir, a aquellos que usan los IED, y que se incluye dentro del planeamiento integral conjunto para la eliminación del adversario «como un todo», actúe donde actúe. Es necesario olvidar la creencia de que una postura pasiva apoyada exclusivamente en robustas medidas de FP va a disuadir al adversario del intento de emplear IED, y aun pudiendo llegar a disuadirle en una acción puntual no va a contribuir a su derrota en el marco general de la operación.

Aportaciones de una fuerza naval

La interdicción marítima constituye el vector fundamental del ataque a las redes (AtN) en el entorno marítimo. Mediante la ejecución de abordajes, las unidades navales pueden evitar el transporte de componentes IED por vía marítima, pueden atacar algunas vías de financiación del oponente, romper sus líneas marítimas de apoyo logístico, evitar el movimiento de terroristas o insurgentes por mar e impedir al oponente la ejecución de tareas de vigilancia (16). No obstante, la interdicción marítima también apoya directamente al pilar de anulación del dispositivo (DtD) y a la base de conocimiento e inteligencia (U&I), gracias a la investigación de posibles WBIED y a toda la reco-

(15) Casi exclusivamente orientado a las medidas de Protección de la Fuerza (MFP).

(16) Todas estas acciones inciden en la actuación de un sistema IED que opera «en y desde la mar», es decir, que lo ataca directamente sea o no el entorno marítimo el área principal de sus ataques. Hoy en día las operaciones marítimas y terrestres en el litoral no pueden considerarse de manera aislada, puesto que ambas están interrelacionadas y se influencian entre ellas en ambos sentidos.

Abordaje *dhow*. (Foto: *www.armada.mde.es).*

pilación de información que se pueda obtener de estos abordajes. Pero para poder aprovechar convenientemente todas las aportaciones de los abordajes a la campaña global C-IED, los trozos de visita y registro (TVR) que participen en estas misiones deberán estar adaptados a la ejecución de algunos cometidos específicos. Estas capacidades adicionales podrían lograrse mediante la disponibilidad de cuatro paquetes de misión que se activarían temporalmente para una determinada unidad: paquete AIT *(Advanced Interdiction Team)* para permitir la ejecución de registros destructivos o microrregistros (17), así como para explotar toda la información que se incaute en soporte físico y digital, efectuar interrogatorios a personal clave y obtener la información necesaria para apoyar la generación de TECHINT *(Technical Intelligence)* y FABINT *(Forensic And Biometric Intelligence);* paquete EOD (18) para poder neutrali-

(17) Los registros destructivos son aquellos que incluyen el desmontaje de mamparos, falsos techos y otros componentes de la estructura interna de un buque; en cambio, los microregistros son aquellos en los que se utilizan fibroscopios o videoscopios para inspeccionar espacios no accesibles.

(18) Las unidades EOD *(Explosive Ordnance Disposal)* son aquellas que llevan a cabo la detección, identificación, evaluación sobre el terreno, neutralización, recuperación y desactivación final de explosivos.

zar un WBIED; paquete WIT (19) para poder explotar en el nivel 1 un incidente IED, y paquete SOF *(Special Operations Force)* para ejecutar abordajes con oposición.

Una aportación fundamental de las fuerzas navales al C-IED en el entorno marítimo es la realización de misiones ISR (20) para apoyar los objetivos de inteligencia de la operación. Y en este contexto cobran especial relevancia las misiones SIGINT (21) —que aportan una información especialmente relevante para los pilares AtN y DtD— y de I&W (22), mediante las cuales se puede llegar a alertar de la ejecución inminente de un ataque. Una fuerza naval dispone de múltiples plataformas, más o menos discretas y con mayor o menor autonomía, para poder ejecutar con eficacia todos estos cometidos de inteligencia: aeronaves tripuladas (ala fija o helicópteros), no tripuladas (UAS) (23), unidades de superficie, submarinos y fuerzas de operaciones especiales. Esto va a proporcionar una flexibilidad enorme y una amplia cobertura sobre los componentes del sistema IED sobre los que se desee establecer la vigilancia.

Además del MPE (24) que se realice en los abordajes y de las misiones ISR que se ejecuten, el ciclo MSA *(Maritime Situational Awareness* o conocimiento del entorno marítimo) es el tercer elemento sobre el que se sustenta la base de conocimiento e inteligencia (U&I) del C-IED en el entorno marítimo. El objetivo de este ciclo es obtener la superioridad de la información en dicho entorno mediante el intercambio de información entre múltiples actores y agencias, y por ello el MSA se convierte en una herramienta indispensable de la estrategia marítima C-IED. Aprovechar la morfología del ciclo MSA y toda la experiencia que han acumulado las marinas aliadas durante los últimos años

---

(19) Los equipos WIT *(Weapons Intelligence Team)* son aquellos que realizan la explotación sobre el terreno (nivel 1) de un incidente IED (STANAG 2298).

(20) *Intelligence Surveillance and Reconnaissance*.

(21) La inteligencia de señales (SIGINT, *Signal Intelligence*) está relacionada con la interceptación de comunicaciones (COMINT, *Communication Intelligence*) y de otras emisiones electrónicas (ELINT, *Electronic Intelligence)*.

(22) Las misiones I&W *(Indications and Warning)* consisten en tratar de identificar una serie de indicadores que están relacionados directamente con la ejecución de una determinada actividad por parte del adversario.

(23) Sistemas aéreos no tripulados *(Unmanned Aerial Systems)*. También es habitual referirse a ellos como UAV *(Unmaned Aerial Vehicles)*.

(24) MPE *(Materiel and Personnel Explotation)* es un proceso sistemático de recopilación de información que se apoya en cuatro pilares básicos: el análisis de documentos tanto en soporte físico como digital, los interrogatorios de carácter táctico, la inteligencia técnica (TECHINT, y la inteligencia biométrica y forense (FABINT). Esta información recopilada se procesará convenientemente y se diseminará en forma de productos de inteligencia. Debe tenerse en cuenta que en el entorno de C-IED, la obtención de TECHINT dentro del concepto MPE está completamente vinculada a los WIT *(Weapons Intelligence Teams)*. Para más información consultar el AJP-3.15 (B) (NATO Unclassified).

debe ser una de las prioridades para adaptar la base de conocimiento e inteligencia (U&I) a las particularidades del entorno marítimo.

Otra contribución de las fuerzas navales al esfuerzo C-IED global está directamente relacionada con la vigilancia marítima, que debe entenderse como la exploración sistemática o no sistemática del entorno marítimo mediante la ejecución de patrullas, búsquedas o reconocimientos. La vigilancia marítima puede implicar a todo tipo de plataformas navales (buques, submarinos, aeronaves y guerra naval especial) y, aunque su objetivo principal siempre estará relacionado con la detección de riegos y amenazas, también va a aportar un valioso componente de disuasión frente al oponente. El simple posicionamiento de unidades navales para obtener un determinado efecto físico o cognitivo puede proporcionar una notable ventaja en la campaña global de la operación. No obstante, a mayor presencia naval, mayor número de blancos se le ofrecen al oponente.

Además de la interdicción marítima y de la vigilancia marítima, existen dos tipos de operaciones de seguridad marítima (MSO, *Maritime Security Operations)* con las que una fuerza naval puede hacer importantes aportaciones al C-IED en este entorno, especialmente al pilar DtD: la protección de infraestructuras críticas y de las líneas de comunicación marítima. Considerando que más del 80 por 100 del comercio mundial y más del 60 por 100 en el caso de la energía son transportados por vía marítima (25), y teniendo en cuenta el elevado número de infraestructuras críticas que se encuentran en el litoral, se puede deducir la importancia que tienen estas misiones dentro de la estrategia C-IED marítima. Además de escoltar el tráfico vulnerable y vigilar rutas y zonas de interés, puede ser de gran utilidad el empleo de todas las herramientas NCAGS *(Naval Cooperation And Guidance for Shipping)* disponibles en beneficio de la comunidad mercante.

La ejecución de operaciones de información en la mar o desde la mar, entre ellas las operaciones psicológicas (PSYOPS) y de KLE *(Key Leader Engagement)*, puede jugar un papel fundamental en el pilar de ataque a las redes (AtN). A pesar de que tanto el objetivo como los medios disponibles son prácticamente los mismos que en el entorno terrestre, la ejecución de estas actividades en el litoral presenta una serie de particularidades que es necesario destacar. A pesar de la movilidad que tiene una fuerza naval y de las ventajas que esto puede implicar para algunas acciones tanto cinéticas como no cinéticas (26), la mar también supone una importante barrera física para la ejecución de todo este tipo de actividades. Además, la selección de la audiencia para estos productos puede resultar compleja, sobre todo si tenemos en cuenta

(25) *www.armada.mde.es*.

(26) Se ha decidido utilizar las palabras «cinético» y «no cinético» como la mejor traducción de los términos *kinetic*, que se refiere a las acciones en las que se emplean medios físicos

la internacionalización de la comunidad mercante y la dispersión de los actores que pueden resultar implicados. Por último, se deberán explotar al máximo las visitas consensuadas y aproximaciones amistosas a los buques y embarcaciones de la zona como vectores para la divulgación de la campaña de información. Una fuerza naval posicionada frente a las costas del oponente también puede efectuar ataques selectivos en tierra para neutralizar elementos clave del sistema IED, como campos de entrenamiento, nodos C2, centros de apoyo logístico, combatientes, etc., o también para provocar efectos psicológicos deseados en el oponente. Para ejecutar esta proyección del poder naval en tierra una fuerza dispone de cuatro vectores principales, que combinados entre sí y gracias a la movilidad que les caracteriza a todos ellos pueden tener efectos decisivos en la campaña militar: aviación naval embarcada tanto de ala fija como rotatoria, misiles de crucero, fuego naval de apoyo y unidades de Infantería de Marina.

Veamos a continuación las aportaciones de una fuerza naval al pilar «anulación del dispositivo» (DtD), vinculadas directamente a la protección de la fuerza. Dentro de ellas se deben citar con carácter general las operaciones MCM y todos los procedimientos MFP contra amenazas de perfil suicida en la mar, y con un carácter más específico las tareas EOD submarinas (UW-EOD) y EOD sobre la superficie (AW-EOD). Sin duda alguna, la mayoría de estas medidas y procedimientos son habituales en las marinas modernas desde hace muchos años, pero algunas necesitan modernizarse con las nuevas tecnologías y adaptarse a la amenaza específica de WBIED. Especial mención merecen la necesidad de avanzar en las tareas EOD sobre la superficie, aprovechando las sinergias entre los equipos EOD y los TVR y profundizando en su integración orientada a la misión, y la de desarrollar la capacidad WIT de explotación de un incidente IED en el entorno marítimo, que está relacionada directamente con cualquiera de las cuatro aportaciones anteriores.

Por último, conviene señalar la importancia de las actividades que las fuerzas navales pueden llevar a cabo dentro del apoyo a la reforma del sector seguridad de un país anfitrión y que estarían encuadradas dentro del pilar de Preparación de la Fuerza (PtF). Normalmente las fuerzas navales proporcionarán este apoyo desarrollando MSO para la consecución de un entorno marítimo seguro y estable, y contribuyendo al desarrollo o construcción de una capacidad naval en el país anfitrión que le permita hacerse cargo de la seguridad y defensa de sus propias costas y aguas.

(misiles, proyectiles, etc.) con resultados letales y no letales, y *non kinetic*, que abarcaría aquellas acciones de carácter etéreo y que se caracterizan por el empleo de medios no materiales (guerra electrónica, ciberataques, operaciones de información, acciones judiciales, acciones económicas, etc.), orientadas a debilitar la voluntad del adversario o impedir sus actividades.

Vigilancia. (Foto: colección del autor).

Desafíos tecnológicos y necesidades materiales

Uno de los campos con mayor potencial para el desarrollo tecnológico en la lucha C-IED es el de la Guerra Electrónica, tanto en el segmento radar como en el de comunicaciones. La capacidad ESM (27) tiene una aplicación directa en el conocimiento del entorno (SA, *Situational Awareness)*, en las alertas sobre la ejecución de un ataque (comunicaciones entre atacantes, señales de control para un RC-WBIED (28), etc.) y en la localización de objetivos potenciales (centros de mando y control, campos de pruebas de IED, etc.). Y si sobre esta vigilancia del espectro electromagnético se aplica el correspondiente nivel de análisis, se puede obtener una SIGINT de elevado valor para

(27) En relación a las medidas empleadas, la Guerra Electrónica se divide en tres grandes bloques: ESM *(Electronic Support Measures)*, ECM *(Electronic Counter Measures)* y EPM *(Electronic Protective Measures)*.

(28) *Radio Control Water Borne* IED: aquellos WBIED iniciados por el atacante mediante dispositivos de radio control (incluidos los sistemas de telefonía móvil).

los pilares AtN (mensajes entre componentes de las redes IED, patrones de conducta del oponente, etc.) y DtD (referencias para la programación de inhibidores). Pero para ser efectivos, todos estos sistemas de guerra electrónica deberán estar adaptados al entorno (densidad electromagnética en el litoral), a la plataforma (operación desde buques o aeronaves navales) y muy especialmente a la amenaza (sistemas de control de un RC-WBIED, dispositivo de iniciación de un WBIED, telefonía móvil, dispositivos portátiles de comunicaciones, etcétera).

La capacidad ECM puede jugar también un papel muy importante, especialmente en lo relativo a perturbación y neutralización. En el primer caso destacan los inhibidores de todas aquellas señales relacionadas con un IED, tanto para proteger a una unidad (FP-ECM) como a los desactivadores que puedan estar actuando sobre el dispositivo (EOD-ECM) (29). Y dentro del término neutralización se encuentran incluidas todas aquellas armas de tecnología avanzada, principalmente HEL (láser de alta energía capaz de destruir un objetivo de pequeñas dimensiones) o HPM (microondas de alta potencia que pueden llegar a detener una embarcación) (30). También son interesantes otros sistemas relacionados con la utilización del espectro electromagnético, como las armas no letales de energía dirigida (ADS (31) o A3D) (32) o los dispositivos de radiodifusión para la ejecución de PSYOPS.

Otro de los segmentos tecnológicos con un marcado interés para la lucha C-IED es el relativo a los equipos de inspección. En primer lugar, se necesitan sistemas avanzados para que un TVR pueda registrar a fondo un mercante o su carga, por lo que el empleo de sistemas de rayos X, de radares de penetración o de videoscopios puede ser algo imprescindible para una unidad con capacidad AIT. Por otra parte, será necesario disponer de detectores de explosivos, tanto analizadores de vapores como de muestras materiales, así como de otro tipo de sistemas equivalentes, pero siempre adaptados al entorno marí-

---

(29) FP-ECM *(Force Protection-Electronic Counter Measure)* y EOD-ECM *(Explosive Ordnance Disposal-Electronic Counter Measure)*. Ambos conceptos están contenidos en el AJP-3.15(B) *Allied Joint Doctrine for Countering Improvised Explosive Devices* (NATO Unclassified). También es muy común encontrar el término CREW *(Counter Radio-controlled IED Electronic Warfare)* y que se puede considerar una terminología «informal», pero extendida en los Estados Unidos para referirse a las FP-ECM.

(30) Para más detalles sobre las armas HEL *(High Energy Laser)* y HPM *(High Power Microwaves)*, se puede consultar el capítulo sexto («Armas de tecnología avanzada», autor Julio Ortega García) del Cuaderno de Estrategia núm. 153 (*Proliferación de las armas de destrucción masiva y de tecnología avanzada*) del IEEE.

(31) ADS *(Active Denial System)*. Para más información consultar *jnlwp.defense.gov o www.globalsecurity.org*.

(32) A3D *(Aversive Audible Acoustic Device)*. Para más información consultar *www.pica.army.mil*.

timo (p. e., un detector de cables terrestres no tendría mucha utilidad a bordo de un buque) (33).

La capacidad MPE (Material and Personnel Exploitation) es otra de las líneas en las que es necesario avanzar y profundizar, así como en la necesaria base legal que la ampare. En primer lugar destacan los equipos para la recogida de datos biométricos, mediante los cuales se pueden tomar huellas dactilares, escanear retinas y capturar imágenes faciales (BATS, HIIDE, SEEK (34), etc.). Estos sistemas deberán ser pequeños y estar «rugerizados», y es especialmente importante que sean interoperables con diversas bases de datos y permitan la transmisión de información en tiempo real al buque que aborda (35). Asimismo, será necesario contar con dispositivos especiales para la recogida de todo tipo de huellas forenses (dactilares, biológicas, balísticas y especiales) como parte de la investigación científico-técnica que se realiza en el lugar del hecho y la cual es siempre irrepetible. Y para completar el resto de aspectos de la MPE, también sería interesante disponer de los sistemas necesarios para la explotación de toda aquella información que se pueda incautar tanto en soporte físico como digital, así como todos los relacionados con la producción de TECHINT (Technical Intelligence), la cual tiene una notable importancia en la lucha C-IED (36). Por último, se debe destacar que todos estos sistemas están relacionados directamente con la capacidad WIT para explotar un incidente IED, sobre la que el Estado Mayor de la Defensa ya emitió un documento de Requisitos de Estado Mayor (REM) Conjunto en el año 2012.

En relación a la neutralización de un posible WBIED, cobra especial relevancia la adaptación al entorno marítimo de los equipos de remoción a distancia, no solo por las condiciones ambientales del medio marino, sino

---

(33) A nivel conjunto ya se han empezado a dar los primeros pasos en este sentido con el documento de Requisitos de Estado Mayor (REM) Conjunto sobre los equipos de búsqueda militar.

(34) Todos los aquí señalados son dispositivos portátiles para la toma de datos biométricos, y que se encuentran en servicio desde hace algún tiempo en muchos países aliados: BATS (*Biometric Automated ToolSet*), HIIDE (*Hand-held Interagency Identity Detection Equipment*) o SEEK *(Secure Electronic Enrolment Kit*).

(35) A este respecto conviene destacar el proyecto C3PO *(Coallition End to End Expanded MIO Performance Optimization),* que está siendo desarrollando actualmente por Estados Unidos. Este sistema permite diseminar y compartir en tiempo real información de abordajes mientras los TVR están todavía a bordo de los buques objetivo. El sistema se basa en una estructura CIS que permite el intercambio de información entre todas las agencias implicadas y en una serie de periféricos mediante los cuales se introduce en dicha red toda la información que el TVR haya recopilado en la escena de acción (datos biométricos, investigación criminal, etcétera).

(36) Para más información acerca de la aplicación del concepto MPE en las actividades C-IED se recomienda consultar el documento *White paper for countering IEDs in the maritime domain* del *Allied Command Transformation* (NATO Unclassified).

por las singulares características de los buques, con cubiertas llenas de obstáculos y espacios muy restringidos en los que es muy difícil operar con estos vehículos no tripulados. Por otra parte, para aquellos IED de carácter submarino y especialmente en teatros alejados donde no haya disponibilidad de una fuerza MCM (37), se debe destacar la importancia de los UUV (38), que junto con otros sistemas aerotransportados (RAMICS, ALMDS o AMNS (39)), conforman la espina dorsal del nuevo concepto de MCM orgánicas.

Por último, merece la pena señalar todos aquellos avances tecnológicos que si bien no son exclusivos del C-IED en el entorno marítimo, sí que pueden jugar un papel determinante como elementos de la lucha contra la amenaza asimétrica: sistemas de detección de última generación (radares, sonares y sistemas electroópticos), montajes de pequeño calibre operados remotamente, vehículos no tripulados (UAV y USV) (40) y materiales que proporcionen una especial protección contra impactos y explosiones.

Síntesis

A pesar de la realidad de la amenaza de empleo de IED en el entorno marítimo, la actitud de las fuerzas navales se sigue manteniendo en un carácter defensivo que no ataca la raíz del problema. La existencia de un marco doctrinal marítimo que acompase las aportaciones de una fuerza naval al esfuerzo C-IED de carácter global y conjunto podría actuar de catalizador para cambiar esta tendencia en el marco de la Alianza. No obstante, se están dando los primeros pasos a todos los niveles y se está empezando a tomar conciencia de la necesidad e importancia de que las fuerzas navales contribuyan con sus cometidos al ataque a las redes IED allá donde existan y actúen.

Las fuerzas navales pueden realizar grandes aportaciones a todos y cada uno de los pilares de la estrategia C-IED, pero la vigilancia y la interdicción marítima, las misiones ISR navales, el ciclo MSA y la proyección selectiva del poder naval en tierra son los principales vectores navales a utilizar en el

---

(37) *Mine Counter Measures*.

(38) UUV *(Unmanned Underwater Vehicles),* los cuales pueden dividirse en tres grupos principales: ROV *(Remotely Operated Vehicles)*, SUV *(Supervised Underwater Vehicles)* y AUV *(Autonomous Underwater Vehicles)*. Fuente CN MORENO SANMARTÍN, Jorge Juan: *La tecnología dual y las medidas contra minas (www.asesmar.org)*.

(39) Todos ellos son sistemas MCM instalados en helicópteros de la familia *SH-60*: RAMICS *(Rapid Airborne Mine Clearance System)*, ALMDS *(Airborne Laser Mine Detection System)* y AMNS *(Airborne Mine Neutralization System)*. Fuente TN HERNÁNDEZ LLOBREGAT, Francisco: *MCM orgánicas*

(40) *Unmanned Surface Vehicle* (USV).

ataque a las redes IED, que es el pilar clave y decisivo en la lucha contra esta amenaza.

Seguramente sea en el aspecto del recurso de material para la lucha C-IED desde y en el entorno marítimo donde se presentan ciertos desafíos tecnológicos, si bien ninguno de ellos es esencialmente novedoso y casi todos resultan adaptaciones navales de sistemas y dispositivos que ya son utilizados o se están desarrollando para otro entorno. El oponente utiliza los avances tecnológicos para mejorar sus sistemas IED, utilizando estos de forma simple y sencilla, y eso mismo deberían hacer las fuerzas militares para poder hacerles frente con mayor eficacia y mejores resultados.