



Puente de mando del BMP 'Cartagena', desde el que se hicieron las pruebas. ANTONIO GIL / AGM

# La Armada prueba con éxito un sistema de guerra híbrida ideado por un oficial del S-81

El teniente de navío Hoyos testa en un ejercicio real novedosos métodos de ataque cibernéticos que desarrolla para su tesis doctoral en la UPCT

GREGORIO MÁRMOL



CARTAGENA. A finales del pasado noviembre, buques mercantes que navegaban por el mar del Alborán comprobaron cómo por unos instantes sus sistemas de navegación, sus comunicaciones por radio y sus servicios sateli-

tales se volvían locos. En esas aguas estratégicas y de gran interés para los intereses españoles la Armada desarrollaba las maniobras Marborán-25, enfocadas al adiestramiento en guerras electrónica y antisubmarina, con la participación de buques como las fragatas 'Blas de Lezo' y 'Numancia' y el submarino 'Isaac Peral' (S-81). Más discretamente, desde el buque multipropósito (BMP) 'Cartagena', probaba con éxito nuevos recursos tecnológicos desarrollados para la guerra híbrida por el teniente de navío Guillermo Hoyos. Ese oficial de la dotación del S-81 se halla embarcado también en una tesis doctoral para ampliar conocimientos y horizontes sobre nuevas tecnologías y sistemas de información relaciona-

dos con la guerra electrónica y más en particular con la guerra de la navegación (en inglés, Navigation Warfare, según la terminología de la OTAN).

En ese concepto se enmarcan aquellas acciones o medidas tecnológicas para asegurar la superioridad de una unidad naval frente a otras en el posicionamiento, la navegación y las señales de referencia de tiempo. Unas se aplican para proteger los sistemas de navegación de un buque y otras para perturbar los de los adversarios.

Los mercantes que aquel día de noviembre vieron alterados



El oficial Hoyos, en la UPCT. LV

diendo y ampliando conocimientos en un campo que será cada vez más relevante en el futuro». Así define el oficial Guillermo Hoyos,

sus sistemas de navegación no fueron los únicos afectados por el ensayo de las teorías de Hoyos. Los radares de las unidades participantes en las Marborán-25 registraron, además, una flota fantasma de hasta 16 barcos ficticios creados mediante equipos de guerra electrónica del BMP 'Cartagena'. La simulación fue posible gracias a la aplicación tecnológica de los planteamientos realizados por Hoyos para su tesis, centrada en mejorar las capacidades militares para reconocer y efectuar perturbaciones en señales de navegación. El desarrollo va orientado a proporcionar a España nuevas capacidades ofensiva y defensiva. Pero eso tardará algún tiempo en fraguar, ya que la propuesta del oficial requerirá mayor análisis procedimental antes de su posible implantación, si finalmente interesa a la Armada.

«Fue un ejercicio de enorme utilidad», explicó hace unos días el marino e ingeniero en la presentación de retos tecnológicos de la Cátedra Jerónimo de Ayaz de la Armada en la Universidad Politécnica de Cartagena (UPCT). Las herramientas que desarrolla permiten simular trayectorias, velocidades y ubicaciones erróneas o inexistentes de buques en los sistemas AIS usados globalmente para la identificación automática de barcos. El ejercicio incluyó rumbos de choque para probar engaños en sistemas de alerta convencionales.

## Señales falsas

La investigación parte de la vulnerabilidad de los sistemas de identificación que carecen de mecanismos de verificación adicional y de su exposición ante ataques electrónicos. De ahí que durante las maniobras se ensayara el sistema de perturbación, que logró afectar a los equipos de navegación civil. Por contra, los equipos militares preparados para esta nueva modalidad de enfrentamiento naval mostraron solvencia reconociendo el ataque.

El uso de señales falsas para distorsionar la información sobre la navegación «es ya un patrón» habitual en la guerra híbrida, según Hoyos. Estas prácticas, denominadas 'spoofing', de las que los rusos son grandes especialistas, se dan masivamente desde 2024 y afectan no solo al

## LA TESIS

► **Título.** 'Técnica de Operación Deceptiva en el Dominio Marítimo: una aproximación desde la Information Warfare'.

► **Autor.** TN Guillermo Hoyos, jefe de Control del Buque en el S-81 'Isaac Peral'. También es ingeniero mecánico con posgrados en Seguridad, Defensa, Geoestrategia y Tecnología de la Información. Además de la tesis doctoral, estudia un máster en Seguridad de la Información y Ciberseguridad.

tráfico marítimo. También al aéreo. Uno de los casos más conocidos trascendió en septiembre pasado: el ataque mediante interferencias al GPS del avión que trasladaba a Bulgaria a la presidenta de la Comisión Europea, Ursula Von der Leyen.

Falsear la señal GPS es lo que logra el transceptor desarrollado por Hoyos, cuya tesis dirigen los profesores de la UPCT María Teresa Martínez Inglés y José María Molina García-Pardo y el de la UMU Humberto Martínez Barberá. Ha probado también a simular falsas derrotas y el uso de un dron de superficie diseñado por el profesor Martínez Barberá para indicar ubicaciones erróneas de buques. Y ha desarrollado un software para multiplicar las señales engañosas que 'apagan' los sistemas AIS para la toma de decisiones.

«Se puede perturbar al adversario únicamente con la información que recibe, no hace falta un misil», explica, para resaltar de las dimensiones cibernética y cognitiva en la nueva doctrina naval. Y sobre el impacto de ambas explica de manera elocuente: «Podemos pensar en situaciones recientes, como el apagón eléctrico ocurrido durante 2025 en España. Más allá de la causa real, lo relevante fue la percepción inmediata de la población: la duda, la incertidumbre y la rápida especulación. Ese efecto sobre la percepción y el comportamiento colectivo es precisamente el tipo de fenómeno que estudia la Information Warfare y que obliga a replantear doctrinas, procedimientos y formación, tanto en el ámbito militar como en el civil».

## Hoyos: «Es un campo que será cada vez más relevante en el futuro»

G. M. P.

CARTAGENA. «Lo que despertó mi interés por la Information Warfare fue comprender cómo las nuevas tecnologías y los sistemas de información influyen cada vez más en el ámbito militar, geoestratégico y táctico, no solo desde un punto de vista técnico, sino tam-

bién desde el impacto que generan en la percepción y en la toma de decisiones. Mi motivación principal ha sido seguir profundizando en un área todavía en evolución, con procedimientos operativos en proceso de definición, y que presenta un alto grado de incertidumbre. A ello se suma una inquietud personal por seguir apren-

de 31 años y gaditano de Chicla de la Frontera, su motivación por ampliar conocimientos en la llamada Information Warfare o guerra de la información.

Su tesis en elaboración, explica, no debe entenderse como el desarrollo de un equipo o un sistema cerrado, sino como un estudio conceptual y académico, apoyado en experimentación controlada, que analiza cómo determinados sistemas de información pueden ser utilizados como herramientas de influencia y engaño en el dominio marítimo.

Acerca de su futura implantación, explica: «Las actividades realizadas hasta el momento han tenido como objetivo validar conceptos y equipos en escenarios abiertos controlados. No se trata de un sistema listo para su implantación operativa, ya que se requiere de un análisis procedimental para su empleo en unidades navales». En esta fase inicial, la investigación se centra en el empleo ofensivo de esas técnicas para conocer el fenómeno en profundidad, añade. El análisis defensivo ser hará en posteriores fases.