Premios Revista EJÉRCITO 2025

Artículos Ganadores

MINISTERIO
DE DEFENSA

Premios Revista EJÉRCITO

2025

Artículos Ganadores

Catálogo de Publicaciones de Defensa
publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA

SUBSECRETARÍA DE DEFENSA

SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

© Autor y editor, 2025

NIPO 083-25-064-9 (edición impresa)

NIPO 083-25-065-4 (edición en línea)

Depósito legal M 20244-2025
Fecha de edición: octubre 2025
Maqueta e imprime: Imprenta Ministerio de Defensa

Las opiniones emitidas en esta publicación son de exclusiva responsabilidad del autor de la misma.

Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del copyright ©.

En esta edición se ha utilizado papel procedente de bosques gestionados de forma sostenible y fuentes controladas

ÍNDICE

PRÓLOGO 7

FALLO DE LOS PREMIOS 9

ARTÍCULOS GANADORES 11

PRIMER PREMIO 13

SEGUNDO PREMIO 23

TERCER PREMIO 31

PRÓLOGO

La Revista «Ejército», fundada el 30 de septiembre de 1939, es la publicación profesional militar del Ejército de Tierra. Tiene como finalidad facilitar el intercambio de ideas sobre temas militares y contribuir a la actualización de conocimientos y la cultura de Defensa. Su larga tradición, como foro y repositorio de pensamiento militar es de un gran valor para el Ejército de Tierra.

La Revista «Ejército» es una publicación oficial del Ministerio de Defensa (MINISDEF) y, por tanto, incluida en su Programa Editorial. La misma no constituye un ente orgánico, sino que es un producto elaborado por la Sección de Publicaciones, de la Subdirección de Servicios de Asistencia Técnica (SUBAT), de la JCISAT.

La Revista «Ejército» es uno de los medios de comunicación más destacados que dan soporte al Sistema de Comunicación del Ejército y, por tanto, al estar integrada en el mismo, contribuye significativamente a la proyección tanto interna como externa, de la imagen de un ejército moderno, preparado, eficaz y al servicio de España. A la vez que se mantiene como un foro de opinión sobre temas técnicos profesionales, de seguridad, defensa, cultura e históricos.

Los «Premios Revista Ejército», cuya creación se remonta a 1980, tienen por finalidad distinguir a los autores de los mejores trabajos y colaboraciones publicados en la Revista durante el año anterior a su concesión y propiciar la creación literaria referida a las múltiples actividades del Ejército de Tierra español en el marco de las Fuerzas Armadas, así como su conocimiento y divulgación.

A continuación, se exponen los artículos que han sido galardonados con los «Premios Revista Ejército» en su XLV edición.

V. — OTRAS DISPOSICIONES

PREMIOS

Resolución 516/12199/25

Cód. Informático: 2025017933.

Resolución del Jefe de Estado Mayor del Ejército de Tierra, por la que se publica el fallo del Jurado «Premios Revista Ejército 2025».

PREMIOS REVISTA EJÉRCITO 2025.

Fallo de la convocatoria.

Premios Revista Ejército 2025 convocados por Resolución 516/08830/25, de 8 de mayo («BOD» núm. 116, de fecha 17 de junio de 2025), de la Jefatura de Estado Mayor del Ejército.

Reunido el Consejo de Redacción de la Revista, constituido como Jurado Calificador y presidido por el General Director Don Manuel Maldonado Pardo, con arreglo a las Bases de la Resolución citada se acuerda:

Primero. Conceder el primer premio, dotado con dos mil novecientos euros (2.900 euros), al General de Brigada de Infantería Don Zacarías Hernández Calvo, por el artículo «La trinchera tecnológica: Israel y su Línea Maginot», publicado en el número 989 correspondiente a marzo/abril de 2024.

Segundo. Conceder el segundo premio, dotado con dos mil euros (2.000 euros), al Coronel de Artillería retirado Don Carlos Tejeda Fernández y a Doña Elizabeth Manzo Carreño, escritora y empresaria, por el artículo «Irán y Hamás ¿Gambito de Dama?», publicado en el número 988 correspondiente a enero/febrero de 2024.

Tercero. Conceder el tercer premio, dotado con mil quinientos euros (1.500 euros), al Coronel de Transmisiones Don Francisco José Oliva Bermejo, por el artículo «Operaciones electromagnéticas en la Guerra de Ucrania», publicado en el número 989 correspondiente a marzo/abril de 2024.

Cuarto. Conceder diploma acreditativo al Doctor en Seguridad Internacional, Máster en Relaciones Internacionales y Licenciado en Sociología y Ciencias Políticas y de la Administración Don Guillem Colom Piella, para reconocer su destacada y dilatada labor de colaboración con la Revista.

Madrid, 18 de julio de 2025.—El General de Ejército JEME, Amador Fernando Enseñat y Berea.

CVE: BOD-2025-157-23001
Verificable en https://sede.defensa.gob.es/acceda/bod

ARTÍCULOS GANADORES

1.º

La trinchera tecnológica: Israel y su línea Maginot

Zacarías Hernández Calvo
General de brigada de Infantería

2.º

Irán y Hamás ¿gambito de dama?

Carlos Tejeda Fernández
Coronel de Artillería retirado

Elizabeth Manzo Carreño
Escritora y empresaria

3.º

Operaciones electromagnéticas en la guerra de Ucrania

Francisco José Oliva Bermejo
Coronel de Transmisiones

PRIMER PREMIO

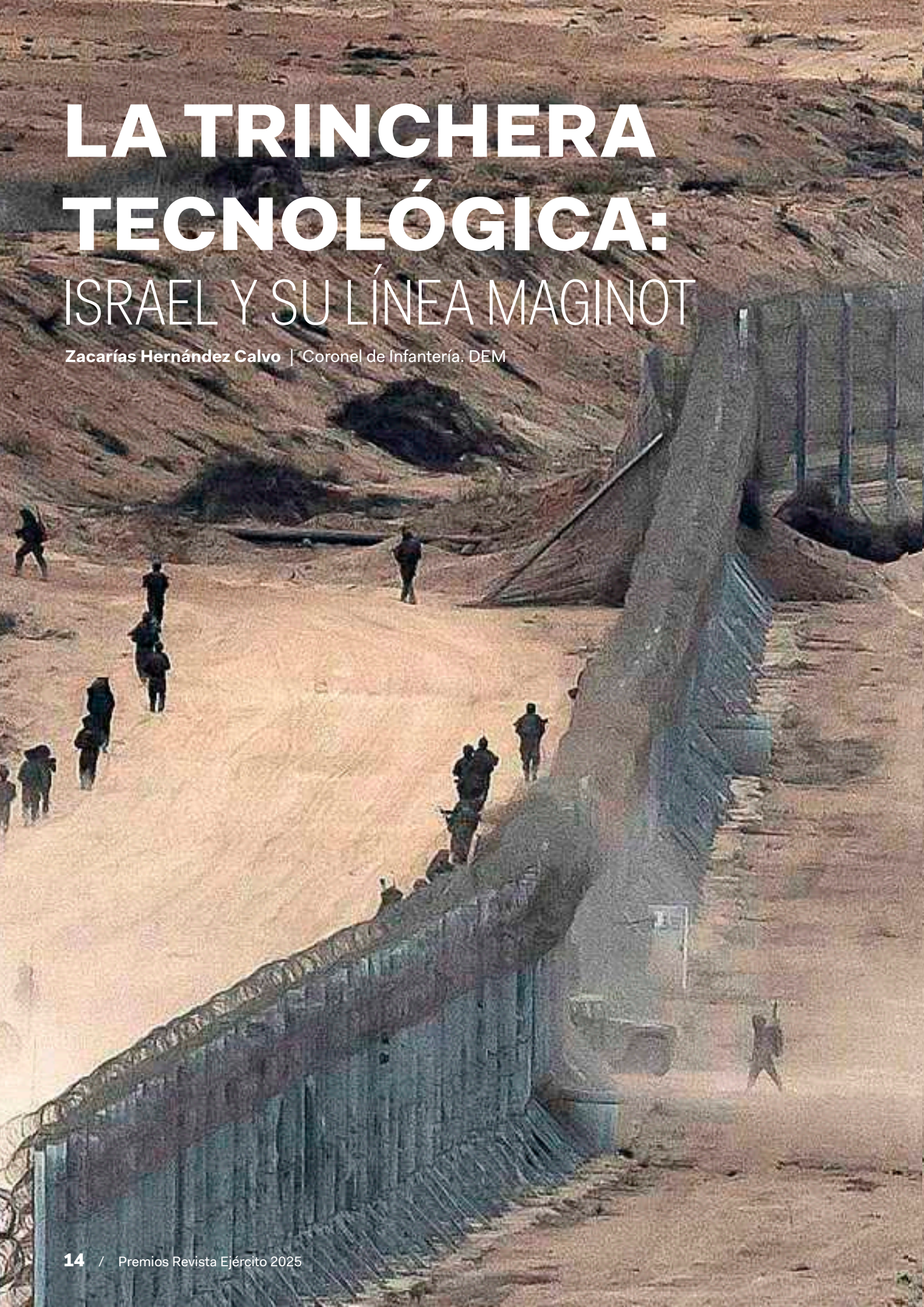
La trinchera tecnológica: Israel y su línea Maginot

Zacarías Hernández Calvo

General de brigada de Infantería

LA TRINCHERA TECNOLÓGICA:
ISRAEL Y SU LÍNEA MAGINOT

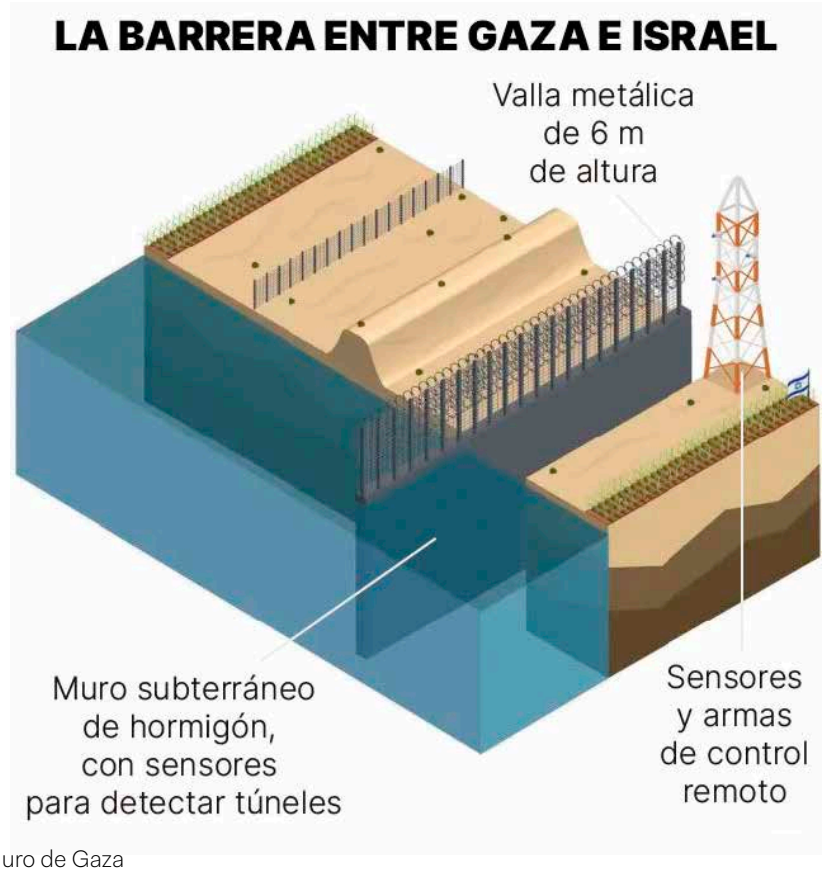
Zacarías Hernández Calvo | Coronel de Infantería. DEM



Cuando el 7 de octubre la organización terrorista Hamás atacó Israel cogió por sorpresa a las Fuerzas Armadas de Israel (IDF). La población israelí y sus fuerzas armadas confiaban en la muralla defensiva de última tecnología recientemente terminada alrededor de GAZA y en su escudo antimisiles conocido como Iron Dome. Al igual que la población francesa hacen más de 60 años con la Lína Maginot, confiaban que las últimas tecnologías en defensa les protegían.

En 1940 como en 2023 las suposiciones fallaron. Demostrando una vez más que cuando se opone la tecnología a un enemigo con voluntad de vencer el ingenio humano prevalece. El pródigo uso que las IDF hacen del próspero sector tecnológico israelí, las permite disponer de alta -y cara- tecnología, que incluye equipos de última generación en sistemas de defensa aérea y antimisiles, cazas furtivos, así como capacidades avanzadas de inteligencia, vigilancia y reconocimiento (ISR).

Sin embargo, la dependencia excesiva de la tecnología puede, en determinadas circunstancias, actuar como un peligroso obstáculo para lograr los objetivos esperados. Cuando las ventajas tecnológicas se degraden, se nieguen, se destruyan o simplemente no sean capaces de alcanzar los objetivos políticos en la guerra, la tenacidad y el ingenio humano para adaptarse seguirán siendo el arma más eficaz y la última línea de defensa.



Muro de Gaza

LA HISTORIA SE REPITE, O POR LO MENOS SE PARECE MUCHO

Construida a lo largo de la frontera oriental de Francia tras la Primera Guerra Mundial, la línea Maginot fue un conjunto de fortificaciones de hormigón, obstáculos y armas construida en la década de 1930 para disuadir de la invasión de Alemania. En el momento de su construcción fue considerada una de las innovaciones más importantes en materia de defensa nacional. Contaba con vías férreas subterráneas que la hacían invulnerable a la artillería y los carros de combate, y disponía hasta de aire acondicionado para las tropas estacionadas. Otorgaba al pueblo francés un confortable sentido de la protección. Los ejércitos alemanes eludieron la línea Maginot en 1940, optando por la línea de acción más impensable: penetrar hacia el norte a través del bosque densamente arbolado de las Ardenas con divisiones acorazadas y una ferocidad alarmante. Toda Europa —incluida Alemania— se vio sorprendida y esta costosa maravilla defensiva del siglo XX se convirtió en un despropósito.

El 7 de diciembre de 2021 Israel anunció la finalización de un muro subterráneo que se extendía aproximadamente sesenta y cinco kilómetros a lo largo de toda la Franja de Gaza. Invirtió tres años y mil millones de euros en esta barrera. Se convirtió en uno de los proyectos de ingeniería más complejos y avanzados jamás realizados en el país. Incluye una barrera subterránea con sistemas de detección, otra en la superficie con tecnologías de vigilancia, sistemas de armas teledirigidas integrados en un avanzado sistema de detección con radares, cámaras de máxima cobertura y salas de mando y control equipadas con inteligencia artificial. En palabras del ministro de Defensa israelí: «La barrera, que es un proyecto innovador y tecnológicamente avanzado, priva a Hamás de una de las capacidades que trató de desarrollar»[1].

Las sofisticadas capacidades de Israel hacen de Gaza, el sur del Líbano y Cisjordania una de las zonas más vigiladas del mundo. Esta barrera terrestre se complementa con uno de los mejores sistemas de defensa aérea. Con una eficacia del 90 %, el famoso Iron Dome proporciona una parte de un sistema de defensa aérea más amplio que también incluye los sistemas David's Sling y Arrow para amenazas de alcance medio y largo. Todo este entramado tecnológico daba a la población de Israel una confortable sensación de protección.

En la madrugada del 7 de octubre, Hamás optó por una línea de acción impensable: lanzó miles de cohetes contra Israel en un día festivo. Sus fuerzas especiales (conocidas como la Nukhba) desplegaron escuadrones de drones equipados con cargas explosivas y granadas que atacaron puestos de guardia y sistemas de vigilancia, control, comunicación y armamento de las Fuerzas de Defensa de Israel (IDF) cerca de la frontera. Algunos equipos se infiltraron en el país por aire, utilizando paramotores.

Línea de Maginot

Iron Dome

Ataque Hamas

Ataque Hamas

Ataque Hamas

A continuación, miles de terroristas de Hamás consiguieron atravesar la frontera en múltiples puntos utilizando artefactos explosivos e infiltrarse en territorio israelí, al estilo del Estado Islámico (EI), en motocicletas y docenas de furgonetas cargadas con armamento diverso, incluidos fusiles, ametralladoras, armas contracarro y un número considerable de granadas de mano.

Queda mucho tiempo para que se puedan analizar en profundidad los aciertos de Hamás y los fallos cometidos por los israelíes el pasado 7 de octubre: problemas en el sistema de inteligencia israelí, subestimación de la capacidad enemiga, innovación táctica de Hamás, sorpresa operacional/estratégica o probablemente, siguiendo la teoría del queso suizo de James T. Reason, la coincidencia o convergencia de múltiples factores. Este artículo pretende explorar el factor del «fetichismo tecnológico» que sufren las IDF y todos los Ejércitos occidentales.

ISRAEL Y LA SUPERIORIDAD TECNOLÓGICA

Como todos los Ejércitos occidentales, recientemente, en 2019-2020, las IDF lanzaron dos publicaciones importantes: *The Momentum Multiyear Plan* y un documento conceptual, *The operational concept for victory*. Ambas pretendían imprimir un cambio significativo en la forma en que las IDF se ven a sí mismas y a sus adversarios. Identifican una necesidad de cambio determinada por dos factores fundamentales: la comprensión de un enemigo difuso definido con el término *rocket-based terror armies* y el aprovechamiento de las nuevas oportunidades que ofrecen los recientes avances de la revolución digital.

Desde su creación, Israel ha perseguido la adquisición de la superioridad tecnológica. David Ben-Gurión, primer ministro y ministro de Defensa, declaró poco después de la creación del Estado de Israel que, debido a su inferioridad numérica, debían esforzarse por lograr una superioridad cualitativa sobre sus potenciales adversarios. Israel consideró que la ciencia y la tecnología eran fundamentales para llevar a cabo esta estrategia.

Iron Dome

Mando y control en vehículo

Puesto de Mando *de Inteligencia Israelí*

Las IDF, construidas en torno a un sistema de servicio militar universal y de reserva, está considerado uno de los mejores Ejércitos del mundo. El pródigo uso que hacen del próspero sector tecnológico israelí les permite disponer de alta —y cara— tecnología, que incluye equipos de última generación en sistemas de defensa aérea y antimisiles y cazas furtivos, así como capacidades avanzadas de inteligencia, vigilancia y reconocimiento (ISR).

A lo largo de los años, esta estrategia se ha convertido en una piedra angular de la identidad de Israel como nación tecnológicamente avanzada, lo que le ha valido el apodo de *start-up nation*, y se ha incardinado significativamente en la percepción de su seguridad nacional. Esta percepción se refleja en la innovadora industria de defensa del país y en el elevado número de nuevas empresas tecnológicas en este sector. Los vínculos con las IDF desempeñan un papel fundamental para la industria israelí de alta tecnología. La mayoría de los ciudadanos realizan el servicio militar obligatorio y muchos continúan en la reserva activa. Existe, por tanto, una interacción continua entre los ámbitos civil y militar israelíes. Esta conexión permanente permite a los empresarios que prestan servicio a las IDF introducir nuevas tecnologías e idear soluciones que pueden contribuir a la defensa.

Continuando el camino que señala Hew Strachan de que «la estrategia después de 1945 puede haber sido materialista, en el sentido de que respondía a la innovación tecnológica más de lo que lo había hecho en el pasado y puede haber utilizado la teoría de juegos y la probabilidad más que la experiencia y los principios», la percepción de que la tecnología puede conducir al dominio militar alcanzó su punto culminante a principios de la década de 1990 con la aparición del concepto de «revolución en asuntos militares» (RMA). Esta idea postulaba que la superioridad militar se basa en soluciones tecnológicas avanzadas para hacer frente a una amplia gama de amenazas y escenarios. El estado de la tecnología permitía impulsar un cambio drástico y decisivo. Esto no solo afectaría a la superioridad de la fuerza militar, sino que tendría el potencial de alterar el equilibrio geopolítico

a favor de los que dominaban la nueva forma de guerra. Con origen en los pensadores soviéticos, el concepto se desarrolló en los círculos de defensa estadounidenses e influyó en las estrategias de varios Ejércitos occidentales, incluido el de Israel. Las décadas de 1990 y 2000 configuraron la visión del mundo de las IDF y de la casi totalidad de los Ejércitos occidentales y la forma en que han percibido la realidad desde entonces. Sin embargo, no podemos dejar de comprender que estas décadas representan un momento relativamente raro en la historia militar de dominio casi total de los Ejércitos occidentales avanzados, particularmente de Estados Unidos.

En esta dirección, uno de los objetivos últimos de los sistemas tecnológicos avanzados israelíes, como en el resto de los países occidentales, es proporcionar una imagen operativa completa y en tiempo real del campo de batalla en cualquier momento. Para alcanzarlo, se han desarrollado medios capaces de ver a través de muros o bajo tierra, sistemas de detección avanzados capaces de proporcionar una cobertura continua del campo de batalla las veinticuatro horas del día, técnicas de gestión de datos mejoradas y métodos de transmisión más eficaces para grandes volúmenes de datos. Además, incluye la utilización de inteligencia artificial para la toma rápida de decisiones, basada en el gran volumen de datos recopilados.

UNA VEZ MÁS, LA REVOLUCIÓN EN ASUNTOS MILITARES (RMA)

Como en un reciente documento señalaban los analistas de defensa israelíes Ofer Shelah y Carmit Valensi,

> *Israel disfruta de una ventaja hasta el punto de una completa unilateralidad en plataformas aéreas y blindadas, inteligencia y municiones de precisión, y ha desarrollado doctrinas de combate influenciadas por la revolución en asuntos militares (RMA), un término general para los cambios drásticos en la naturaleza de la guerra debidos a los avances en las armas precisas y de largo alcance, la informática y la guerra centrada en redes.*

APC Eitan

Smash Smart Shooter

Iron sting

Los cambios en la formación y el empleo de las fuerzas de las IDF en las últimas décadas crearon las capacidades y el concepto operativo que posteriormente se utilizó en la campaña de entreguerras[2]: el énfasis en la inteligencia de alta calidad que permite ataques precisos; operaciones aéreas que permiten ampliar el radio de acción de las operaciones, actuar con precisión y evitar bajas entre las fuerzas israelíes; y municiones de precisión que permiten, en la medida de lo posible, evitar daños colaterales a los no combatientes.

El principal reto, tal y como las IDF lo han interpretado en las últimas décadas, estaba en las limitaciones que se habían autoimpuesto y no en las capacidades del enemigo. Sin embargo, puede que sea precisamente esta búsqueda de las IDF de una superioridad tecnológica sobre adversarios de menor nivel, como Hamás, lo que ha nublado su visión.

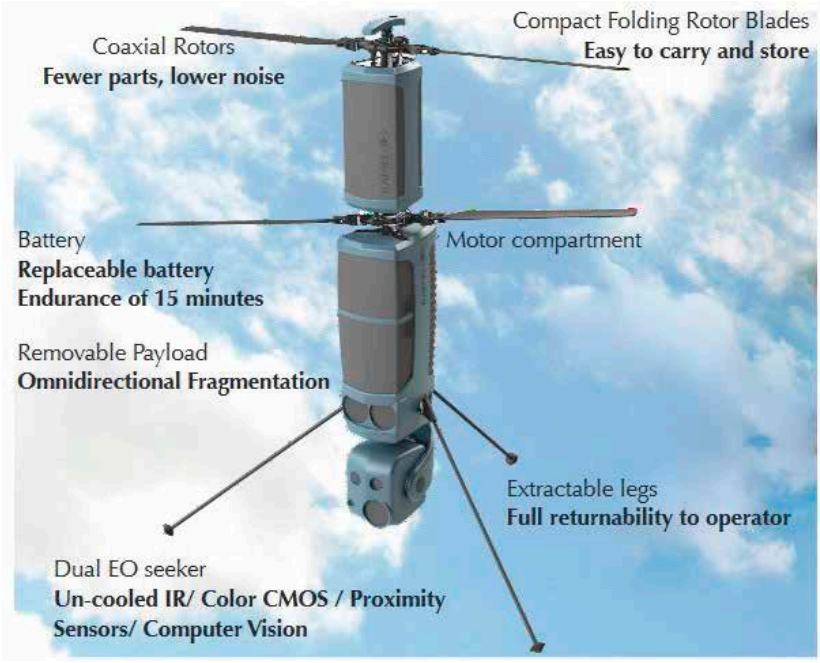
Ya en la década de 1990 se observaron signos preocupantes que indicaban que el camino por el que se avanzaba no daba los resultados esperados. Se producía una erosión de la supremacía aérea de Israel. La superioridad en los fuegos era una premisa básica de la RMA. Todas las campañas de las IDF durante la década de 1990 se caracterizaron por combates con costes humanos y económicos crecientes y ataques cada vez más frecuentes en el frente interno israelí. Sus decepcionantes resultados solían atribuirse a los consabidos desafíos de las campañas de contrainsurgencia. La aparente paradoja entre la supremacía de las IDF y los ambiguos resultados de las campañas, particularmente contra Hizbulá, causaron frustración entre los responsables de la toma de decisiones y la opinión pública israelí.

Un importante aviso llegó durante la segunda guerra del Líbano, en la denominada operación Just Reward. La nueva doctrina operativa de las IDF, publicada en abril de 2006, tres meses antes de la ofensiva, estaba muy orientada a la tecnología. Predicaba el predominio de la potencia de fuego sobre la maniobra y se centraba en la consecución del éxito en el campo de batalla mediante una combinación de fuego preciso y operaciones limitadas sobre el terreno, la necesidad de influir en el ámbito cognitivo del enemigo, el papel central desempeñado por la aviación y la disminución de las maniobras terrestres a gran escala y en profundidad. Todo ello bajo las complejas teorías de las operaciones basadas en efectos.

Las IDF no completaron la misión antes de que se produjera el alto el fuego. A pesar de conseguir algunos éxitos tácticos, fracasaron en alcanzar resultados decisivos en el campo de batalla contra Hizbulá, es decir, en negar la capacidad del enemigo para seguir combatiendo. El sistema descentralizado de mando y control de Hizbulá permaneció intacto, lo que favoreció el resultado final. El jefe del Estado Mayor de las IDF, Dan Halutz (Ejército del Aire), destacó la principal razón de las dificultades de las IDF en el campo de batalla: la tendencia de los altos mandos a dirigir la lucha no al frente de sus tropas en el campo de batalla, sino desde sus cuarteles generales, situados en la retaguardia, confiando excesivamente en la tecnología. Conducir la guerra a través de pantallas de plasma podía ser compatible con la suposición de que, en un campo de batalla donde las fuerzas enemigas son destruidas por fuego de precisión, el mando y el control óptimos se logran desde los centros de control. Lo que les había faltado a las IDF en aquella guerra era un sistema de mando sencillo. «Se puede dirigir un McDonald's con pantallas de plasma, pero no una batalla», dijo.

El 7 de octubre la tecnología volvió a no ser suficiente. Israel esperaba cohetes, que llegaron, pero como distracción para permitir el paso a una ofensiva terrestre con buldóceres. El muro resultó inútil porque los parapentes baratos demostraron su eficacia para saltarlo. Israel esperaba que los sistemas de vigilancia detectaran señales de alerta, pero parece que Hamás confió en la forma más antigua de comunicación: la conversación cara a cara. Israel solo permitía a Gaza una red 2G, convirtiéndola indirectamente en su propio talón de Aquiles porque, cuanto más sofisticados son los móviles, mejor funciona el espionaje. Además, pensó que su sistema Iron Dome podía protegerlos, pero la saturación por el lanzamiento masivo de cohetes sobrepasó sus capacidades. Los famosos drones de vigilancia nunca volaron porque Hamás atacó primero las instalaciones del Ejército que albergaban a sus operadores.

La operación Iron Swords se encuentra todavía en desarrollo en el interior de la Franja de Gaza y es difícil sacar conclusiones a estas alturas, pero demuestra los retos a los que siguen enfrentándose los Ejércitos, incorporando tecnología avanzada a las plataformas existentes.



Spike Firefly

Dentro de lo que parece una ofensiva tradicional, Israel ha activado a cientos de miles de reservistas, ha realizado ataques aéreos durante semanas y ha lanzado una invasión terrestre con dos divisiones, incluyendo varias brigadas de infantería, ingenieros de combate y comandos navales, con un gran apoyo artillero. Por supuesto, algunas de las tecnologías más recientes de Israel están siendo utilizadas. Aunque se ha empleado inteligencia artificial y macrodatos para identificar objetivos, las herramientas automatizadas aún requieren de una gran fuerza sobre el terreno para ser útiles. El uso eficiente de equipos de operaciones especiales dirigidos por sensores de inteligencia contra objetivos de alto valor y el sistema de control de disparo Smash (Smartshooter) para el cierre más rápido de los bucles «sensor-tirador» en los fusiles, el sistema de mortero de precisión Iron Sting (Elbit Systems) o el Spike FireFly (Rafael), una munición merodeadora que puede sobrevolar y esperar a que haya un objetivo disponible, también se han utilizado por primera vez en este conflicto. En cuanto a los vehículos, se ha desplegado el APC Eitan, parece que con el sistema de protección activa Iron Fist (Elbit Systems). Muchos vehículos blindados de Gaza están equipados con el sistema de protección activa Trophy (Rafael), aunque hay indicios de que en algunos casos no funcionó como se esperaba. Todos estos sistemas y otros utilizados son parte del Momentum Multiyear Plan y están teniendo un impacto sobre el terreno, pero el ritmo de la campaña muestra que, en general, el cambio que aportan no es disruptivo, sino progresivo.

ENTONCES, ¿QUÉ HACEMOS?

Está muy claro que la tecnología es un multiplicador de fuerza sobre el campo de batalla. Todos los avances tecnológicos deben ser tenidos en cuenta en los niveles estratégico, operacional y táctico. Sin embargo, sus ventajas se quedan en el plano táctico cuando la confianza en la superioridad tecnológica se utiliza como sustituto de la estrategia. Como nos ha demostrado la historia, resulta esencial la capacidad de evaluar los efectos estratégicos de la tecnología para utilizarla en la dirección y el propósito de la guerra. De hecho, existe una relación entre el crecimiento tecnológico y la innovación militar. Debemos competir en el espacio tecnológico. Pero el sesgo tecnológico no debe cegarnos; ya Clausewitz nos advirtió de que, independientemente de la innovación técnico-militar, la guerra es, ante todo, una contienda violenta entre voluntades opuestas que sirven a fines políticos. Cuando el enemigo está en desventaja tecnológica, subirá sus apuestas por la violencia, la voluntad de vencer y la política.

Aunque la superioridad tecnológica es, y probablemente seguirá siendo, un elemento importante del *modus operandi* de las IDF y el resto de Ejércitos occidentales, la experiencia de los últimos años enseña que la clave para ganar una guerra y crear efectos duraderos seguirá estando, probablemente, en el control del territorio. Aunque puede lograrse cierto grado de control por medio de la tecnología, el control total exige una presencia sustancial, a veces masiva, de «botas sobre el terreno», como Estados Unidos aprendió en sus campañas de Afganistán e Irak. Estamos viendo que Ucrania e Israel lo han experimentado. Es poco probable que surja una tecnología milagrosa que cambie esa realidad fundamental. La dependencia excesiva de la tecnología en conflictos puede, en determinadas circunstancias, actuar como un peligroso obstáculo para lograr los objetivos esperados.

Cuando las ventajas tecnológicas se degraden, se nieguen, se destruyan o simplemente no sean capaces de alcanzar los objetivos políticos de la guerra, la tenacidad y el ingenio humano para adaptarse seguirán siendo el arma más eficaz y la última línea de defensa. Más allá del fango de los debates en torno a la guerra híbrida, la ciberguerra, la guerra de robots o las operaciones multidominio, la lección más importante es que nunca hay que oponer la tecnología al ingenio humano porque los humanos acabarán ganando. Las guerras nos han dejado claro que las suposiciones estratégicas pueden ser catastróficas cuando van unidas a la fe en el materialismo estratégico de Strachan o a la creencia de que la estrategia debe responder principalmente a la innovación tecnológica.

NOTAS

1. Ver Reuters: «Israel announces completion of underground Gaza border barrier». Disponible en: https://www.reuters.com/world/middle-east/israel-announces-completion-underground-gaza-border-barrier-2021-12-07/
2. La «campaña de entreguerras» es el término oficial israelí para la serie de acciones ofensivas realizadas, principalmente en territorio sirio, durante la última década. Lo que comenzó como acciones puntuales destinadas a impedir la transferencia de armas desde una Siria en desintegración a la organización Hizbulá en el Líbano evolucionó hacia una campaña a gran escala que ha tomado naturaleza en el concepto operativo militar de Israel, incluso en los documentos de estrategia de las IDF.

BIBLIOGRAFÍA

- Ferguson, Michael P. (04/10/2019). «The digital Maginot line: autonomous warfare and strategic incoherence», en *PRISM*, vol. 8, n.º 2.
- Frantzman, Seth (13/11/2023). «New tech plays role in Gaza war, but not to level Israel once envisioned», en *Breaking Defense*.
- Gady, Franz-Stefan (26/10/2023). «Israel's military tech fetish is a failed strategy», en *Foreign Policy*.
- Kober, Avi (2008). «The Israel defense forces in the Second Lebanon War: why the poor performance?», en *Journal of Strategic Studies*, vol. 31, n.º 1, pp. 3-40.
- Reuven, Nir (20/11/2023). *The limits on technological superiority. BESA Center, Perspectives Paper n.º 2, 234*.
- Shelah, Ofer y Valensi, Carmit (2023). *The campaign between wars at a crossroads. Memorandum n.º 227*. Institute for National Security Studies.
- Strachan, Hew (2005). «The lost meaning of strategy», en *Survival*, vol. 47, n.º 3, pp. 33-54.
- Sullivan, Patrick y Amble John (10/10/2023). «What happened to Iron Dome? A lesson on the limits of technology at war», en *Modern War Institute*. ■

SEGUNDO PREMIO

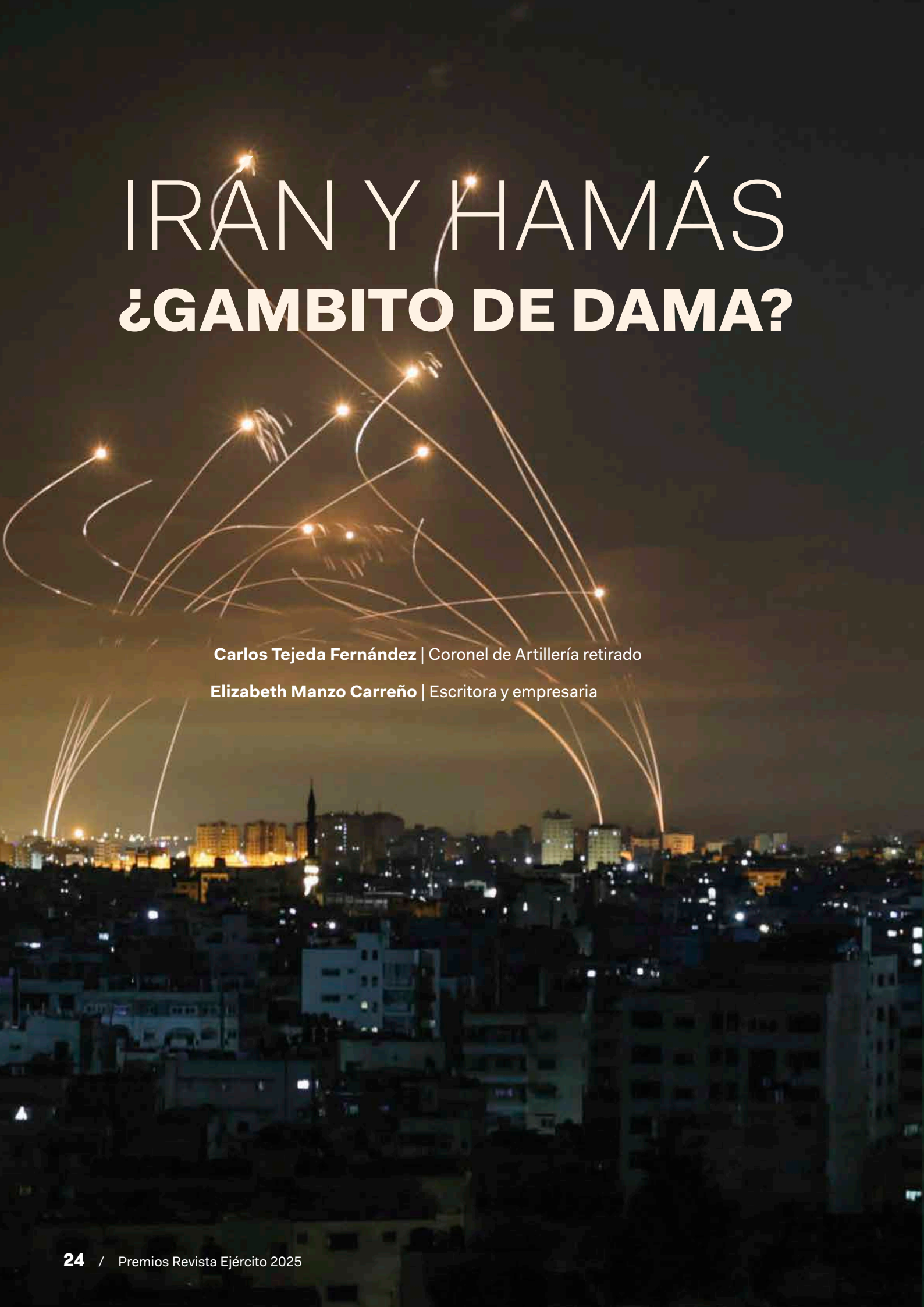
Irán y Hamás ¿gambito de dama?

Carlos Tejeda Fernández

Coronel de Artillería retirado

Elizabeth Manzo Carreño
Escritora y empresaria

IRÁN Y HAMÁS
¿GAMBITO DE DAMA?



Carlos Tejeda Fernández | Coronel de Artillería retirado

Elizabeth Manzo Carreño | Escritora y empresaria

Desde el asalto y el secuestro de la Embajada estadounidense en Teherán el 4 de noviembre de 1979 y la posterior definición del país norteamericano como el «gran Satán», el Gobierno de la República Islámica de Irán no solo no ha buscado la estabilidad de Oriente Medio, sino que probablemente se ha convertido en el mayor desestabilizador de su entorno a nivel mundial.

Como todo régimen nacionalista, teocrático o, en definitiva, alejado del concepto de democracia plena, el país necesita de un alter ego, un enemigo interno o externo que justifique sus fines y procedimientos, por lo que la búsqueda de soluciones diplomáticas no tiene una gran prioridad en su agenda, más allá del propio interés coyuntural y mucho más acá de lo que podría interpretarse como la metodología de su realpolitik.

El régimen iraní, en definitiva, hace muchos años que decidió convertir en enemigos, o casi, a cualquiera de los países occidentales, comenzando —claro está— por los Estados Unidos, y, por supuesto, a Israel, siquiera porque este es el caso paradigmático en el que se centra uno de los principales objetivos de disputa entre la causa de los Gobiernos teócratas de Oriente Medio, de corte mayoritariamente chiita, como Irán.

Los últimos conflictos civiles en Siria e Irak, con una profusa participación persa, y sobre todo las actuaciones de Hizbulá y Hamás, apoyados moral, económica, material y propagandísticamente por Irán, muestran trazas de un «gambito de dama» por parte persa sobre el tablero de Oriente Medio, es decir, de una jugada en la que se sacrifica a la reina (Palestina) para preservar y dar una ulterior victoria a su rey (Irán).

En este punto, por extraño que resulte a la «buenista» filosofía occidental, hay que destacar que ni Hamás ni mucho menos Irán (en este caso, los muertos los pone otro, o sea, Palestina) pretenden limitarse a ganar una guerra a Israel con unos acuerdos justos —o incluso ventajosos— de paz, sino a la total destrucción y desaparición del Estado judío. Irán no lo hace de forma directa (como cuando intervino directamente en Siria, donde sus milicias actuaron encuadradas entre los contendientes chiitas en apoyo de al Asad); pero sí mediante organizaciones declaradas como terroristas, tales como Hamás en Gaza o Hizbulá en el sur del Líbano. Esto hace pensar que en realidad el Gobierno de los ayatolás aún teme al Estado israelí, un ente del que se sabe que es consciente de que, en una hipotética guerra perdida, se juega su supervivencia y que, por tanto, luchará con todos los medios a su alcance; cosa que no hará nadie, ni siquiera Hamás, aunque sí algunos de sus activistas, como se ha demostrado en el día a día a través de atentados suicidas y asesinatos individuales o en masa sobre una población no necesariamente comprometida con la política o la guerra.

Hasta aquí tenemos una panorámica bastante periodística de los hechos que rodean el conflicto en sí, pero hay que considerar que existen claves que van más allá de la simple crónica y que vale la pena evaluar.

Así como cualquier analista de Oriente Medio sabe de la rivalidad entre Pakistán e Irán al este del país, en sus respectivas «zonas de influencia» sobre territorio afgano, más evidente aún resulta la disputa entre el Estado persa y el saudí al oeste de aquel, como demuestra la intervención armada directa en Irak, Siria, el Líbano —con Hizbulá— y ahora, a través de Hamás, en Gaza.

Pero ¿qué hace Irán, país chiita por excelencia, apoyando, adiestrando y armando a los sunnitas de Hamás, es decir, a aquellos a quienes ha combatido en las guerras civiles de los mencionados países?

Para explicar esto, habría que partir de la base de que las grandes jugadas son las que con un solo movimiento alcanzan varios objetivos o al menos producen varias amenazas simultáneamente. Desde el punto de vista iraní, son los dos que se han apuntado: causar el mayor daño al Estado de Israel —por no hablar de su destrucción, algo que comparte con sus peones palestinos— y convertirse en la potencia predominante en Oriente Medio, para lo que necesita incrementar su influencia en el entorno en detrimento de los saudíes, motivo por el que apoya abiertamente a los hutíes (también chiitas) de Yemen, donde trata de menoscabar a las fuerzas aliadas de Riad. Pero existen algunos objetivos adicionales, siquiera de orden secundario...

Alí Jamenei, líder iraní

Carros de combate israelíes en Gaza

En directa relación con todos estos propósitos, cabe traer a colación los «síntomas» que han espoleado a Irán a actuar a través de Hamás. Aunque no se le ha dado demasiada importancia en los medios nacionales, con la notoria mejora de las relaciones diplomáticas entre Israel y algunos países árabes, tales como Marruecos, que —ahora sí— tanto ha dado que hablar por la contrapartida de los servicios prestados al Estado alauí con la utilización del sistema Pegasus, Irán ha percibido el inicio de un acercamiento entre los países árabes más moderados e Israel: una primera señal de alarma para el régimen de los ayatolás, que considera un riesgo de quiebra en el frente común de los países de mayoría musulmana contra Israel.

Pero la cosa no queda ahí: el anuncio por fin de un intento de normalización en las relaciones entre Israel y Arabia Saudí, principal competidor del régimen persa, disparó todas las alarmas en Teherán. Ya no se trataba de un régimen «moderado», sino del más puro «wahabismo» sunnita y del mayor rival regional, eso sí, aliado con el «gran Satán», los Estados Unidos. Por eso, ante la amenaza de que los acuerdos de paz de Abraham con Israel asfixiaran los objetivos estratégicos de Irán en la región, Alí Jamenei, el líder religioso de la república islámica, advertía que «los países islámicos que apuesten por la normalización con Israel perderán», una señal inequívoca de nerviosismo. Y, justo cuando las conversaciones para los acuerdos con la monarquía saudí estaban a punto de iniciarse, se produjo la incursión de los terroristas de Hamás en territorio israelí con los terribles resultados de todos conocidos. Sería de todo punto ingenuo pensar que una acción de semejante calado pudiera llevarse a cabo sin un adecuado planeamiento y un adiestramiento previo, pero ¿por qué precisamente en el momento en el que se produjo?

Seguramente el intento de restablecimiento de las buenas relaciones entre Arabia e Israel tenga mucho que ver, porque cortar toda dinámica de paz entre estos dos rivales del régimen iraní —aunque lo sean por diferentes motivos y puntos de vista— se supone de importancia capital para Teherán. Efectivamente, la esperada y contundente reacción israelí a la hora de aplicar su derecho de autodefensa echó por tierra toda la negociación, que quedó inmediatamente paralizada, siquiera por el «qué dirán» de los países musulmanes que hasta este momento lideraba, al menos moralmente, la monarquía saudita. Así que objetivo conseguido por parte del régimen de los ayatolás en tanto en cuanto los saudíes quedan aislados en su intento de recuperar el camino de una paz duradera con Israel o desacreditados por una supuesta «connivencia» con el enemigo, lo que constituye una especie de chantaje moral.

Otro efecto colateral es el que se produce entre la propia población sunnita de Gaza (y es importante distinguir entre esta y los verdaderos líderes de Hamás, que disfrutan de una vida acomodada en terceros países). Por muy sunnitas que sean, el chiita Irán es el país que los ha armado, adiestrado y lanzado a su incursión en cada uno de los kibutz israelíes asaltados, así que, paradójicamente, los persas ganan enteros frente a los saudíes en la franja sunnita, ahora ocupada por las unidades israelíes.

Dicho esto, aún sería interesante conocer un análisis del impacto que ha tenido la incursión terrorista palestina, auspiciada por Irán, sobre la propia población israelí y su repercusión a nivel mundial.

En primer lugar, el golpe de Hamás no se ha producido en un momento en el que el Gobierno israelí gozara de una gran credibilidad; por el contrario, Netanyahu había sido profundamente cuestionado en fechas anteriores próximas al ataque de Hamás. Esto en la práctica significa que, tras una «reunión del rebaño ante la amenaza del lobo» y la búsqueda de protección en los «perros guardianes» (las fuerzas de defensa de Israel), las disensiones previas comienzan a manifestarse nuevamente e incluso a agudizarse.

Que Hamás haya matado o martirizado a muchos israelíes completamente inocentes, lo que incluye a ancianos, niños y, en general, personas no llamadas a filas o combatientes, o que la retaliación judía haya tenido dimensiones terribles no significa que no haya judíos que preconicen la paz por encima de todo. Junto con la defensa a ultranza del Estado recreado por Ben Gurión, coexiste un cierto pacifismo israelí que, siquiera por cansancio de tanta beligerancia (como lo hay también del lado palestino), propugna otras vías.

En este sentido, hay que tener muy en cuenta a asociaciones promotoras del diálogo y el fin de los enfrentamientos tanto en Israel como en una parte de la población gazatí, aunque aquí en menor medida (pues la sombra de Hamás es alargada), que se han vuelto extremadamente beligerantes con sus propios Gobiernos.

La toma de rehenes israelíes por parte de Hamás ha sido un punto determinante en este conflicto que ha dividido a la población israelí porque ha creado en su población anhelos contradictorios: los familiares, amigos y personas que, por encima de todo, empatizan con los secuestrados piden el fin de las operaciones militares y la apertura de unas negociaciones que permitan su libertad; pero el Gobierno israelí sabe que, si no acaba con Hamás ahora, no alcanzará nunca la paz, cosa que ni aun así estaría garantizada.

Por otra parte, desde el momento en el que Hamás ha excavado cuantiosos kilómetros de túneles, pero también utiliza hospitales, escuelas y otros lugares públicos para establecer sus cuarteles generales o sus depósitos de armas y a la población civil —cuyas muertes y heridas son ampliamente cacareadas ante la prensa internacional como propaganda antiisraelí— como escudos humanos, la dicotomía se reproduce a nivel internacional, y se oyen voces poco realistas que hablan de las barbaridades cometidas por Hamás, pero condenan las acciones emprendidas por Israel en suelo gazatí.

La toma de rehenes israelíes por parte de Hamás ha sido un punto determinante en este conflicto que ha dividido a la población israelí porque ha creado en su población anhelos contradictorios

Ciertamente, el sufrimiento entre la población no combatiente palestina resulta insoportable, pero todas estas voces lo que están pidiendo es una utopía buenista, «un pez grande, pero que pese poco». Por dura que resulte, mucho más explícita y realista es la posición israelí, que se resume en algo como: «No queremos la destrucción de civiles palestinos inocentes, sino solo la de Hamás, pero, si para esto tienen que morir los civiles que se interpongan, morirán antes de que Hamás prevalezca y entonces sean nuestros civiles los asesinados por el grupo terrorista (y no precisamente como víctimas de daños colaterales)».

Netanyahu se lo dejó muy claro al presidente de turno de la Unión Europea en su visita a Israel tras el «inicio» (más bien eterna continuación) del conflicto. Por eso, junto con el clásico dulce et decorum est pro patria mori («dulce y honorable es morir por la patria») de Horacio, Israel ha optado por una frase apócrifa que algunos atribuyen al general Patton: «No se trata tanto de dar la vida por la patria, sino de hacer que el enemigo muera por la suya».

Por supuesto que esta cruda realidad ha chocado con las buenas intenciones de ciudadanos de todo el mundo, lo que los ha hecho unirse a manifestaciones propalestinas, en especial nutridas mayoritariamente por sectores políticos que tradicionalmente han apoyado la causa o se han mostrado manifiestamente antijudíos. Pero, más allá de la ideología revolucionaria, está la realidad de la inmigración de los países árabes y norteafricanos en América y sobre todo en Europa, que, obviamente, ha aumentado la tensión de las manifestaciones contra el Estado de Israel y contra el que les abrió las puertas, pues se considera que este es un aliado de aquel o que no se significa suficientemente en favor de la causa palestina. Téngase en cuenta que existe algún suburbio en París cuya población musulmana está en torno al 80 % de la totalidad y que, en caso de conflicto abierto entre Israel e Irán, muy probablemente habría células terroristas actuando en los Estados Unidos y Europa. Es también por eso muy importante desalojar a Hamás del Gobierno de Gaza para negar su financiación y el apoyo militar de Irán, que ha invertido miles de millones de dólares en este grupo y en Hizbulá a través de la Guardia Revolucionaria iraní. Pero ni aun así existe la certeza de poder erradicar el problema, ya que la organización terrorista posee un entramado internacional que la abastece a través de una compleja trama de negocios fraudulentos, empresas pantalla, organizaciones benéficas, inversiones en criptomonedas de difícil detección y ONG radicadas en algunos países árabes, europeos y de los Estados Unidos y Canadá de las que ni siquiera ISIS dispuso.

Soldado israelí. Fuente; Defensa@Israel

CONCLUSIONES

Irán ha optado por una política imperialista basada principalmente en el liderazgo sobre áreas y países de población significativamente chiita. Esto es especialmente significativo en los casos de Siria, Líbano y Yemen, donde ha intervenido de modo directo. En el caso de Israel, a pesar de su poder armamentístico, Irán aún teme demasiado al país hebreo y las consecuencias de un ataque sobre este tanto por su respuesta militar como por las reacciones internacionales. Por eso se limita a utilizar a otros actores.

Irán trata de convertirse en el principal valedor de movimientos terroristas chiitas, tales como Hizbulá, pero también sunnitas mediante la financiación de Hamás y la consiguiente salida de esta organización de la órbita de su gran rival geopolítico saudí.

Irán se ha beneficiado de que Hamás haya desencadenado su enorme ataque terrorista justo cuando Israel iniciaba conversaciones con Arabia Saudí. Cui prodest?

A través de Hamás, Irán, consciente de la previsible reacción judía, ha golpeado a Israel, pero ha provocado el sacrificio de una gran parte de civiles gazatíes, que sufren un calvario insoportable mientras los dirigentes de Hamás viven y conspiran tranquilamente en algunos de los Emiratos Árabes.

Irán ha propiciado reacciones, a veces violentas, en determinados sectores políticos occidentales, obviando la brutalidad de Hamás y resaltando la enorme destrucción producida por las tropas israelíes en Gaza para ganar la batalla del relato.■

Bandera islamista

TERCER PREMIO

Operaciones electromagnéticas en la guerra de Ucrania

Francisco José Oliva Bermejo

Coronel de Transmisiones

OPERACIONES ELECTROMAGNÉTICAS EN LA GUERRA DE UCRANIA

Francisco José Oliva Bermejo | Coronel De Transmisiones. DEM

Emblema fuerzas EW de la Federación de Rusia

Moscú ha desarrollado, desde el año 2009, un ambicioso programa de modernización de sus capacidades de Guerra Electrónica.

Doctrinalmente integradas con sus capacidades de ciberataque y de guerra de información, constituyen uno de los elementos fundamentales de su estrategia A2/AD *(Anti-Access / Area Denial* o Antiacceso y denegación de área, en castellano).

Con una cuantiosa inversión, la organización de un buen número de unidades y a la formación de su personal, las Fuerzas Armadas rusas tienen capacidad de interferir las comunicaciones, los radares y los sensores OTAN por medio de un amplio catálogo de medios diseñados para contrarrestar las capacidades tecnológicas occidentales y explotar nuestra dependencia creciente del espectro electromagnético.

Sin embargo, tras los combates del último año en la guerra de Ucrania, el nivel de desempeño de estas capacidades ha oscilado entre la total ineficacia y éxitos puntuales, aunque eso sí de elevado impacto mediático.

Se pretende aquí, usando siempre fuentes abiertas, realizar un análisis de los motivos y extraer unas primeras lecciones aprendidas de utilidad para nuestras propias Fuerzas Armadas.

Krasuka 2 ruso con capacidad de interferencia de radares aéreos. Foto: Vitaly V. Kuzmin

El final de la guerra de Ucrania, iniciada en el año 2014 y recrudecida por la invasión de Rusia del 24 de febrero de 2022[1], se antoja aún lejano. Sin embargo, ya es posible extraer lecciones en el ámbito de las operaciones electromagnéticas, que se consideran de interés para nuestras Fuerzas Armadas.

Esta fase nos hace olvidar episodios anteriores como las operaciones electromagnéticas realizadas en las proximidades de Zelenopillya el 11 de julio de 2014 contra la 79 Brigada Aeromóvil ucraniana o en enero de 2015 en Debaltsevo (a escasos cincuenta kilómetros de Bajmut) con los mercenarios de Wagner como protagonistas. En ambos casos, se vio el resultado de la modernización de la guerra electrónica (en adelante EW, *electronic warfare*) rusa desde 2008, que llevó a la creación de las tropas de EW como especialidad independiente en el año 2009 y a su crecimiento bajo el liderazgo del teniente general Yuri Lastochkin.

EL PROGRAMA RUSO DE MODERNIZACIÓN DE LA GUERRA ELECTRÓNICA

La EW es fuente de titulares por la fascinación tecnológica que la envuelve. Sin embargo, sus capacidades pocas veces son entendidas y a menudo se relegan a asuntos de especialistas. Esto es peligroso, teniendo en cuenta que las operaciones electromagnéticas, cuya capacidad troncal es la EW, tienen una importancia creciente y que sus acciones deben coordinarse y sincronizarse con el resto para alcanzar los resultados operativos deseados.

En el caso de la Federación Rusa, la capacidad de EW, conocida como REB (*radioelektonnaia borba*), está diseñada para alcanzar lo que denominan el principio de «superioridad y supremacía electromagnética» e incluye capacidades dirigidas no solo a la degradación de las comunicaciones de radio, sino también a reducir la capacidad ofensiva de sistemas de armas guiadas, radares y sistemas de defensa aérea, así como al control técnico de emisiones propias realizado por sus unidades KTK (*kompleksnyi teckhnicheskii control*). Por ello estaríamos hablando, más que de EW, de operaciones electromagnéticas, ya que también incluyen la gestión del espectro, la inteligencia de señales y la guerra de navegación.

La EW táctica de la Federación Rusa se organiza en brigadas independientes, una por distrito militar, y una compañía por brigada de maniobra, en total unas cuarenta. Dotadas con una extensa panoplia de estaciones, se han identificado más de catorce tipos distintos, por ejemplo, las R-330Zh Zhitel (con capacidad de interferir en comunicaciones de telefonía móvil y satélite y de sistemas GPS), las RB-301B Borisoglebsk-2 (que componen el sistema principal de las compañías de EW y tienen capacidades para la detección y la supresión de comunicaciones HF/VHF, comunicaciones satélite y sistemas de navegación), las RB-341V Leer 3 (equipadas con UAV Orlan-10 diseñados para suplantar redes de telefonía móvil y generar tráfico de mensajes a teléfonos móviles), la RB-531B Infauna (sobre plataforma 8x8 de interferencia de emisores radio y celulares), los Krasukha-4 (antisistemas aéreos diseñados para neutralizar satélites en órbita baja y señales GPS de municiones guiadas) o las Pole-21, con la función de interferir en señales GPS y usadas ya como material fungible.

Al aspecto material se une la formación en el 1084 Centro de Entrenamiento Conjunto en Tambov, que se complementa con la enseñanza en la Academia de la Fuerza Aérea en Voronezh, donde se imparten los cursos de EW y ciberseguridad, y con el adiestramiento en los ejercicios periódicos Elektron, Vostok o de guerra de información Kavkaz.

Como vemos, el esfuerzo y la determinación por dotarse de una capacidad avanzada de EW han sido sostenidos en el tiempo y coherentes en su organización y adiestramiento, y se consideran una pieza clave del desarrollo de la guerra rusa de nueva generación. Pero ¿cuál es el resultado obtenido en Ucrania tras este esfuerzo?

EL DESEMPEÑO DE LA GUERRA ELECTRÓNICA RUSA EN UCRANIA

Además de las evidentes operaciones cinéticas de las campañas de bombardeos, los ataques con misiles o las maniobras de columnas de carros de combate, existen otras acciones que deben analizarse contando con menos fuentes de información fiables, dado el hermetismo que las envuelve. Entre ellas, están las acciones en el ciberespacio, que no debemos confundir con las electromagnéticas —donde se encuadra la EW— y que han llevado al enfrentamiento entre el denominado IT Ukranian Army y las capacidades cibernéticas rusas, tanto de sus servicios de inteligencia como de los grupos de activistas relacionados con ellos.

Igualmente pasan desapercibidas las operaciones electromagnéticas. En este campo, y de acuerdo siempre con información procedente de fuentes abiertas, parece evidente que el rendimiento ruso no estuvo al nivel de las expectativas iniciales. Sin embargo, podemos adelantar que no se

debió a la ineptitud de las unidades de EW rusas, aunque hubiera fallos evidentes, sino a una suma de motivos susceptibles de ser modificados durante el desarrollo de las operaciones, tal y como se está produciendo. Para el análisis de su rendimiento, dividiremos las operaciones en tres fases.

Borisoglebsk–2B destruido en las proximidades de Jersón

Primera fase (de febrero a mayo de 2022)

Aunque el 24 de febrero de 2022 fue el día D de la invasión de Ucrania, las operaciones se habían iniciado con anterioridad. Los ciberataques y la EW sustituyeron la destrucción física de nodos de telecomunicaciones e infraestructuras energéticas. Al ataque no cinético a la infraestructura de comunicaciones satélite de Viasat, mayoritariamente empleada para uso gubernamental, se unió el envío masivo de mensajes a los teléfonos móviles a prácticamente todos los generales y coroneles del ejército ucraniano, instándolos a no combatir y a evitar males mayores a la sociedad ucraniana.

Su efectividad fue contrarrestada por una Ucrania preparada y apoyada por capacidades civiles y militares occidentales. Eso no obvia lo que David Cutler y Daniel Black, el asistente del secretario general y el analista principal de la Cyber Threat Analysis Branch de la OTAN respectivamente, ponían de manifiesto en *Foreign Affairs*: La magnitud de las operaciones cibernéticas destructivas precinéticas de Moscú no tenía precedentes. Las unidades cibernéticas rusas implementaron con éxito tanto *malware* destructivo contra objetivos militares convencionales, la infraestructura de comunicaciones civiles y los centros militares de mando y control como el resto de las potencias cibernéticas del mundo combinadas en un año[2].

Algo parecido sucedió con la campaña de EW que buscaba localizar y suprimir las defensas antiaéreas ucranianas (GBAD, *ground based air defense*). Durante la primera semana de la invasión el *jamming* ruso sobre los sistemas S-300 y los radares SA-11 fue particularmente efectivo, especialmente en Kiev y el eje Hostomel-Irpin[3]. La GBAD ucraniana, durante este periodo, fue suprimida electrónicamente, lo que permitió atacar con medios aéreos más de cien objetivos ucranianos en profundidad. Sin embargo, sus resultados parecen indicar que estas acciones no fueron sincronizadas con las operaciones en curso.

Cuando comenzó la invasión terrestre por múltiples ejes, las unidades de EW rusas acompañaron a los grupos tácticos (BTG, *batalonnaya taktcheskaya gruppa*). La falta de resultados de la EW incluso hizo pensar que se estaban guardando las capacidades por si se escalaba a un conflicto mayor contra la OTAN. Esta percepción no es correcta y se estima que se desplegaron hasta cinco brigadas, tres batallones y dos compañías de EW. La realidad fue que tanto las redes civiles de Internet como la telefonía móvil sobrevivieron al ataque ruso, lo que permitió el enlace del Gobierno con sus Fuerzas Armadas y su población. Sin duda, la falta de integración, la articulación en BTG que carecen de capacidad adecuada para el planeamiento y la conducción de EW y la pérdida de personal clave (como fue el caso del general Andréi Simonov, jefe de EW, en Izium en mayo de 2022) dan pistas sobre los motivos de su pobre rendimiento. Sin embargo, los problemas van más allá.

En primer lugar, Ucrania no era tan débil en el ámbito electromagnético como pensaban. La experiencia de los reveses de 2014 les había enseñado que había que reducir la huella radioeléctrica de sus puestos de mando, dispersarlos y aumentar su movilidad, y las brigadas de EW rusas no fueron capaces de distinguir los emisores propios, civiles en muchos casos, de los ucranianos, muy abundantes en zonas urbanizadas. Ucrania contó con una ayuda occidental en el campo de las tecnologías de sistemas de información y telecomunicaciones nada desdeñable. Así, este apoyo abarca desde el proporcionado por empresas del sector tecnológico (Microsoft, Google o Starlink) hasta la dotación de equipos —como la radio L3Harris RF-7800V Falcon-3— que se enfrentaron con éxito al *jamming* ruso[4].

En segundo lugar, muchos de los medios de telecomunicaciones de dotación en el ejército ruso carecían de las debidas capacidades de protección electromagnética y la falta de medios militares hizo necesario el empleo de *walkies* y teléfonos móviles civiles[5]. Se produjeron tantas interferencias en los medios propios por la falta de medidas de protección y un planeamiento adecuado de los planes de comunicaciones (los conocidos como planes EMCON) que los propios comandantes rusos solicitaron el alto de las actividades de EW en el teatro, lo que supone el «principal fallo de la EW del ejército ruso en el conflicto»[6]. Un ejemplo del *jamming* fratricida fue el sufrido por los pilotos rusos, que, cuando se activó la EW, vieron como se había interferido en sus comunicaciones tierra-aire, al igual que en sus sistemas de navegación y sus radares. Cuando las fuerzas rusas activaron sus *jammers* durante la fase inicial, Ucrania probablemente hizo lo mismo. [...] Todo este *jamming* habría sido agónico para los jefes militares de ambos bandos, pero ¿a quién le hacía más daño? A los atacantes que están intentando moverse y atacar. Las fuerzas defensivas preposicionadas no son inmunes, pero el efecto es mucho menos perjudicial para sus esfuerzos.[7]

Sistema Saniya C-UAS instalado sobre un carro T-80BV

Segunda fase (de mayo de 2022 a febrero de 2023)

En esta fase la concentración de fuerzas en las operaciones realizadas para enlazar Crimea y el Donbás cambiaron la forma y la efectividad del empleo de la EW. Al contrario de los escasos resultados de la primera fase, el uso de la EW en zonas rurales menos pobladas y con menor número de emisiones presentes mejoró. Ya no se hablaba de fracaso, sino que su buen desempeño era destacado como una excepción en el mar de la incompetencia militar rusa.

La eficacia contra los drones ucranianos, cifrada por los analistas del Royal United Services Institute (RUSI), alcanzó el 90 % de efectividad. Entre ellos, los Bayraktar TB-2 turcos demostraron ser vulnerables ante el *jamming* a su guiado por GPS y sus enlaces de datos[8]. A partir de abril, se extendió el uso de UAS Orlan-10 como señuelos para la activación de los SAM ucranianos, que eran inmediatamente localizados por la EW y designados con la rapidez suficiente para ser atacados con misiles o artillería convencional. Sin embargo, esta mejora en el desempeño de la EW tampoco fue definitiva. De nuevo las deficientes comunicaciones rusas las seguían haciendo vulnerables para el combate en el campo de batalla electromagnético. Por un lado, la GBAD rusa se mostró vulnerable a los misiles AGM-88 HARM, pero también lo eran sus comunicaciones tácticas.

En mayo se produjeron los reiterados intentos de cruzar el río Siversky, dirigidos a permitir la captura de los óblast de Donetsk y Lugansk. A la complejidad que supone una operación de paso de río se unió la indiscreción radioeléctrica, que permitió a las fuerzas ucranianas devolver el golpe sufrido en 2014 en Zelenopillya y destruir dos BTG rusos y gran parte de un batallón de pontoneros tras interceptar sus comunicaciones y ejecutar un detallado plan de fuegos integrado con su EW.

El 29 de agosto de 2022 se produjo la contraofensiva ucraniana que llevó a la retirada del frente de Járkov, la liberación de Izium el 10 de septiembre y la retirada al sur del Dniéper, abandonándose la ciudad de Jersón. Se entraba a partir de aquí en una nueva fase de atrición y desgaste centrada en las ciudades de Bajmut, Avdiivka, Marinka y Vuhledar. Destaca entre ellas Marinka, donde en enero de 2023 el empleo indebido de emisiones llevó a la muerte de un centenar de soldados rusos que, deseosos de felicitar el año nuevo, telefonearon a sus familias, permitiendo su localización por parte de Ucrania.

Tercera fase (de marzo de 2023 hasta octubre de 2023)

Las ofensivas ucranianas, en las que se recuperaron extensos territorios en las zonas de Járkov y Jersón, dieron paso a una estabilización de frentes y a una guerra de atrición que se asemeja a la Primera Guerra Mundial.

Evidentemente, las Fuerzas Armadas de Rusia están adaptándose y aprendiendo de sus errores. El despliegue de medios de EW ha ido en aumento, al igual que su dispersión, dada la amenaza y la proliferación de drones ucranianos y el empleo creciente de municiones guiadas, recibidas de la ayuda occidental. La continuidad del frente, su proximidad al territorio ruso, la situación estática y el tempo de las operaciones están permitiendo aumentar la coordinación de las acciones de EW y su sincronización con los fuegos. Todo indica que, reduciendo sus objetivos, están siendo capaces de usar la EW para interferir en las comunicaciones ucranianas sin afectar a las propias[9] desde la primavera de este año. Esto implica que han realizado mejoras en su equipamiento, pero también en las medidas de control y coordinación adoptadas para el uso del espectro electromagnético.

La densidad de equipos de EW rusos desplegados es abrumadora y está demostrando su buen rendimiento al degradar las capacidades de municiones guiadas HIMARS y JDAM norteamericanas, interfiriendo en sus sistemas de navegación, lo que está llevando a modificaciones urgentes en sus sistemas de *software*.

A ello se suma el alto nivel de atrición logrado sobre los UAV ucranianos gracias a los sistemas Zhitel, Krasukha-4 y Moskva-1 y la efectividad al interferir en las comunicaciones de mando y control ucranianas, llegando incluso a romper sistemas de cifrado complejos en tiempo casi real[10].

Esto hace que las contraofensivas ucranianas hayan sido recibidas, junto con el plan de obstáculos, con potentes barreras no cinéticas. Como afirma Dara Massicot, investigadora sénior de la RAND Corporation: «El ejército ruso todavía es capaz de realizar operaciones complejas, realizar un aprendizaje adaptativo y soportar un nivel de combate que pocos ejércitos en el mundo pueden aguantar».

LECCIONES PARA LAS FAS ESPAÑOLAS

Un Ejército aprende de forma intensa durante sus campañas, sobre todo si es capaz de analizar tanto sus victorias como sus derrotas. En nuestro caso esta experiencia operativa se debe adquirir e integrar en la organización y el adiestramiento de las Fuerzas Armadas a través de la identificación de lecciones de conflictos próximos.

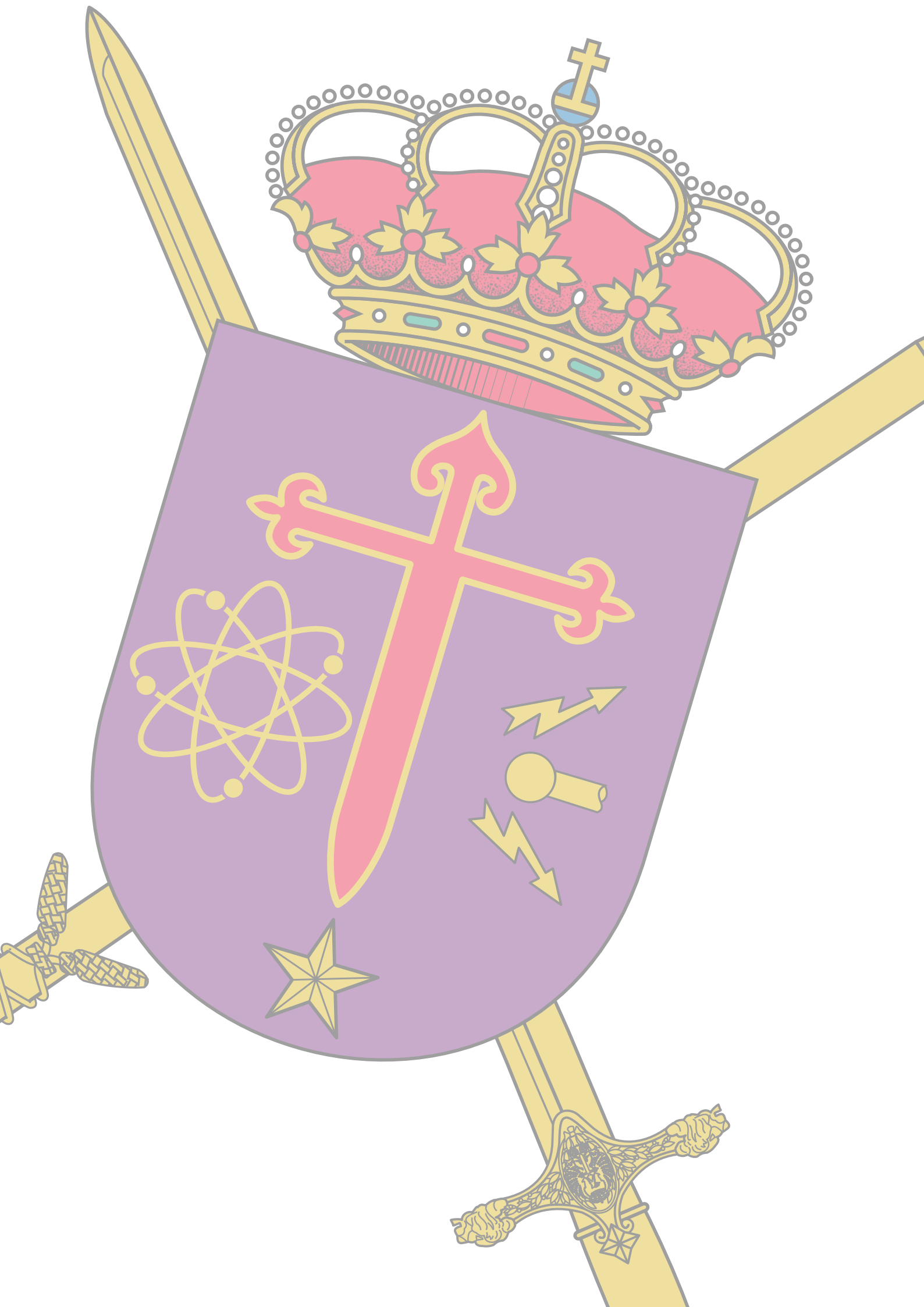
Entre ellas cabe destacar la importancia de la capacidad de EW de la Federación Rusa como parte de su estrategia A2/AD, especialmente diseñada para contrarrestar las capacidades de mando, control, comunicaciones e inteligencia de la OTAN. Debemos pensar que esta capacidad no es solo propia de la Federación Rusa, sino que también, en mayor o menor medida, pueden emplearla otros Estados revisionistas del *statu quo* internacional. El nivel de desarrollo tecnológico alcanzado supera en muchas áreas el occidental y el esfuerzo en su obtención solo puede ser entendido si lo enmarcamos en un ámbito mayor que el de la EW tradicional. La EW es una parte troncal de las operaciones electromagnéticas, que deben entenderse como un elemento clave de las operaciones multidominio. Se debe tener en cuenta que el espectro electromagnético es un medio físico más en el que se desarrollan verdaderos combates con repercusiones directas sobre los ámbitos físico, virtual y cognitivo. Para ello, se debe avanzar de forma decidida en la adopción de medidas de sincronización y coordinación de las operaciones electromagnéticas con el resto de acciones y efectos, impulsar las estructuras de mando y control y los sistemas que las apoyen.

El control de las emisiones propias a través de los planes EMCON es fundamental. Hemos analizado cómo los propios comandantes rusos pidieron que cesaran las acciones de *jamming* al no poder hacer uso de sus propios medios. De nada sirve disponer de capacidades de EW avanzadas si estas no se pueden emplear, ya sea por falta de medios propios adecuados o de una disciplina de empleo. El adiestramiento sin enemigo es peligroso. Por ello nuestras Fuerzas Armadas deben adiestrarse en el uso de sus capacidades tecnológicas en ambientes degradados electromagnéticamente. Por último, el uso de medios de EW y la proliferación de sensores en el campo de batalla hacen que la dispersión, la movilidad y el enmascaramiento (físico y electrónico) sean características imprescindibles en todos los niveles, pero muy especialmente en los vulnerables puestos de mando, los centros logísticos y las propias unidades de EW.

NOTAS

1. Dacoba Cerviño, Francisco José (24/02/2023). Ucrania, nueve años en guerra... por ahora. Documento de Análisis IEEE 15/2023. Disponible en: https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA15_2023_FRADAC_Ucrania.pdf. Consultado el 16/05/2023.
2. Citado en Lin, H. (2022). «Russian cyber operations in the invasion of Ukraine», en The Cyber Defense Review, vol. 7, n.º 4, pp. 31-46. Disponible en: https://www.jstor.org/stable/48703290
3. Bronk, Justin et al. (07/11/2022). The Russian air war and Ukrainian requirements for air defense. RUSI. Special report. Disponible en: https://rusi.org/explore-our-research/publications/special-resources/russian-air-war-and-ukrainian-requirements-air-defence
4. Withington, Thomas (17/05/2022). «Life in the old SINCGARS waveform yet», en Defence and Security Monitor. Disponible en: https://dsm.forecastinternational.com/wordpress/2022/05/17/life-in-the-old-waveform-yet/#:~:text=In %20the %20wake %20of %20Russia %E2 %80 %99s %20invasion %20of %20Ukraine,into %20the %20Ukrainian %20theatre %20of %20operations %20from %202014. Consultado el 15/05/2023.
5. Congressional Research Service (2023). Russia's war in Ukraine: military and intelligence aspects. CRS report. Disponible en: https://crsreports.congress.gov/product/pdf/R/R47068. Consultado el 15/05/2023.
6. Withington, Thomas (16/06/2022). «Russia's electronic warfare capabilities have had mixed results against Ukraine», en The War Zone. Disponible en: https://www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle. Consultado el 15/05/2023.
7. Fischer, Jeffrey H. (13/04/2022). «A key reason for Russia's colossal electronic warfare failure in Ukraine», en The Defense Post. Disponible en: https://www.thedefensepost.com/2022/04/13/russia-electronic-warfare-failure-ukraine/. Consultado el 15/05/2023.
8. Axe, David (24/12/2022). «Russia's electronic warfare troops knocked out 90 percent of Ukraine's drones», en Forbes. Disponible en: https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/. Consultado el 19/05/2023.
9. Massicot, Dara (08/02/2023). «What Russia got wrong», *en Foreign Affaires*. Disponible en: https://www.foreignaffairs.com/ukraine/what-russia-got-wrong-moscow-failures-in-ukraine-dara-massicot. Consultado el 19/05/2023.
10. Watling, Jack y Reynolds, Nick (19/05/2023). Meatgrinder: Russian tactics in the second year of its invasion of Ukraine. Royal United Services Institute for Defence and Security Studies. Disponible en: https://rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine. Consultado el 26/06/2023.■

Soldado ucraniano de la 10 brigada de asalto de montaña Edelweiss operando un Sistema C-UAS en las proximidades de Bakhmu



EJÉRCITO DE TIERRA | LA FUERZA DE LOS VALORES

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL