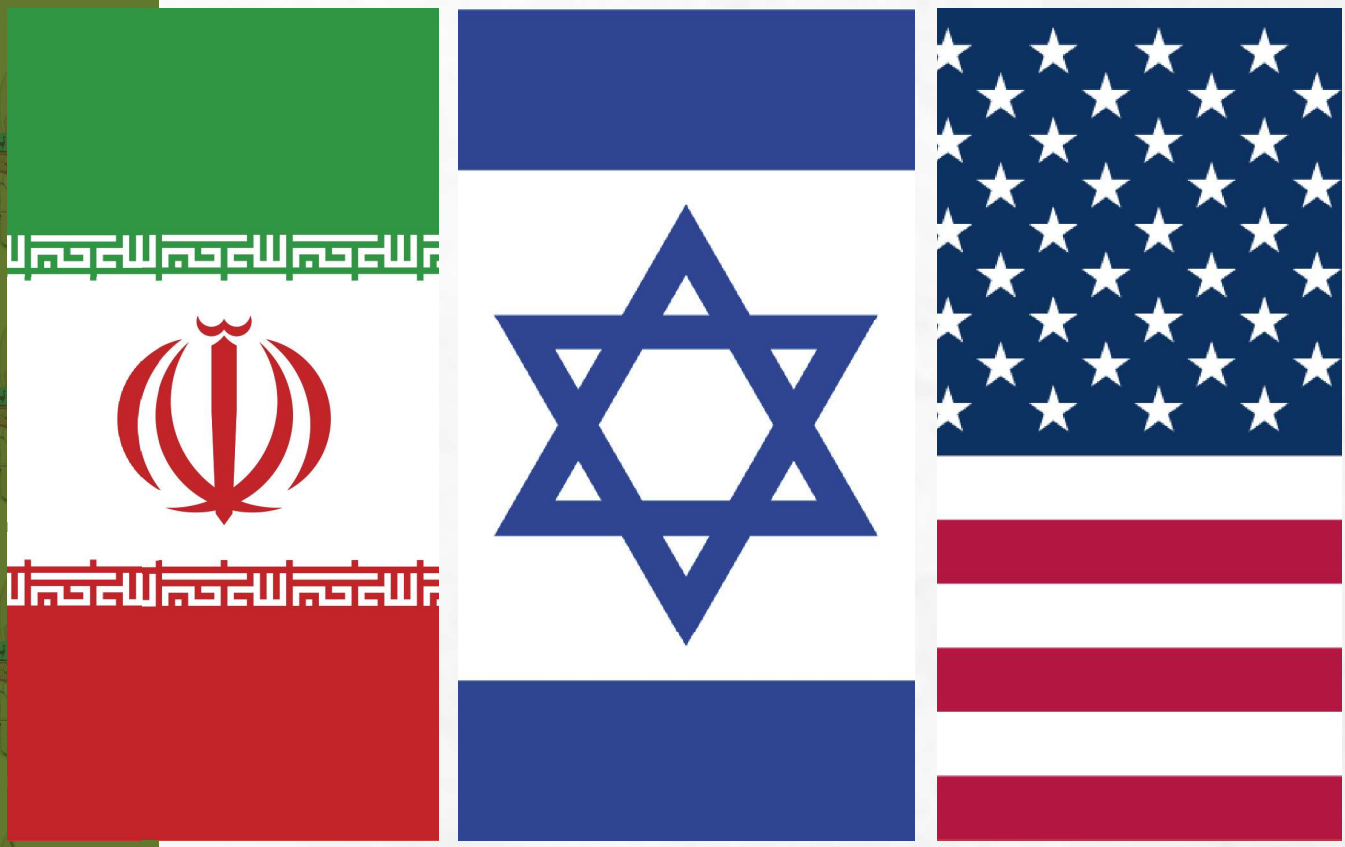
El artículo analiza el conflicto Irán–Israel–Estados Unidos de 2025 como un punto de inflexión en la guerra contemporánea. Examina el empleo de tecnologías emergentes, operaciones multidominio y el papel central de la inteligencia estratégica. El estudio evidencia la consolidación de la guerra de quinta generación, caracterizada por velocidad, interoperabilidad y superioridad informacional. Identifica lecciones clave en disuasión, ética, toma de decisiones y profesionalización militar. Se concluye que la gestión del combate es el eje decisivo del conflicto armado del siglo XXI.

# El conflicto Irán–Israel–EEUU de 2025: Doce (12) días que han redefinido la Guerra Contemporánea



## The 2025 Iran–Israel–United States Conflict: Twelve (12) Days that Redefined Contemporary Warfare

This article analyzes the 2025 Iran–Israel–United States conflict as a turning point in contemporary warfare. It examines the use of emerging technologies, multidomain operations, and the central role of strategic intelligence. The study highlights the consolidation of fifth-generation warfare, characterized by speed, interoperability, and informational superiority. It identifies key lessons in deterrence, ethics, decision-making, and military professionalization. It concludes that combat management constitutes the decisive axis of twenty-first-century armed conflict.

Pimentel, V; Ramos, M.; Guzmán, A. (2025). El conflicto Irán–Israel–EEUU de 2025: Doce (12) días que han redefinido la Guerra Contemporánea. Revista *Pensamiento Conjunto*, Año 13, N° 2. pp. 100-112. ISSN° 2707-367X

Fecha de recepción: 13 de octubre de 2025.
Fecha de aceptación: 16 de diciembre de 2025.
Fecha de publicación: 31 de diciembre de 2025.

***Coronel EP***
***Víctor Manuel Pimentel Roque***
**orcid.org/0000-0002-3511-1996**

*Licenciado en Ciencias Militares, Magister y Doctor en Administración. Cuenta con maestría concluida en Desarrollo, Investigación e innovación tecnológica y otra en Planeamiento Estratégico para el Desarrollo. Especializado en planeamiento estratégico, inteligencia estratégica, gestión de inversiones, gestión pública, docencia universitaria, metodología de investigación, análisis de escenarios, doctrina e historia militar.*
*Ganador del III y V Concurso Nacional de Historia Militar (2007 y 2010); premio "Ejército del Perú – Estímulo a la investigación, desarrollo e innovación en Ciencia y Tecnología" (2022) y ganador, por dos años consecutivos (2024 y 2025), del Concurso de Historia - Nivel investigadores en el Centro de Estudios Histórico Militares del Perú.*
*Actualmente se desempeña como Jefe de Gestión Patrimonial e Inversiones en el Comando General de Apoyo al Ejército del Perú.*

## 1. INTRODUCCIÓN

El conflicto interestatal (CAI) que tuvo lugar entre Irán, Israel y Estados Unidos durante julio de 2025 marcó un hito significativo en la evolución de los conflictos armados contemporáneos. A diferencia de crisis regionales anteriores, esta confrontación de doce (12) días se caracterizó por una escalada rápida, el empleo sistemático de tecnologías emergentes (como sistemas autónomos de combate, drones hipersónicos y plataformas de guerra electrónica avanzada), así como por una coordinación táctica de alta precisión entre actores aliados. La disponibilidad de inteligencia multidominio en tiempo real y la integración operativa entre fuerzas aéreas, cibernéticas y espaciales convirtieron este conflicto en un laboratorio de ensayo para las capacidades de combate del siglo XXI (Al Jazeera, 2025; The Jerusalem Post, 2025).

Este artículo desarrolla un análisis contextual de los hechos principales que marcaron el desarrollo del conflicto, examina las tácticas innovadoras y los sistemas de armas empleados, y plantea una reflexión estratégica orientada a extraer lecciones relevantes para la formación, alistamiento y readaptación del personal militar frente a los desafíos de una guerra de quinta generación (Fifth generation of warfare - 5GoW), donde la velocidad, la interoperabilidad y la superioridad informacional definen el resultado de las operaciones.

**PALABRAS CLAVE:** GUERRA DE QUINTA GENERACIÓN, OPERACIONES MULTIDOMINIO, DISUASIÓN ESTRATÉGICA, INTELIGENCIA ARTIFICIAL MILITAR, GESTIÓN DE COMBATE.
**KEYWORDS:** FIFTH GENERATION WARFARE, MULTI-DOMAIN OPERATIONS, STRATEGIC DETERRENCE, MILITARY ARTIFICIAL INTELLIGENCE, COMBAT MANAGEMENT.

***Mayor EP***
***Eyson Manuel***
***Ramos de la Cruz***

*Egresado de la Escuela Militar de Chorrillos perteneciendo a la 118a Prom. - "Mariscal Eloy Gaspar Ureta Monte Hermoso". Operador Especial Comando, con habilidades extremas en combate, liderazgo y operaciones en diversos terrenos bajo estrés. Jefe de patrulla en la lucha contra el narcoterrorismo en la zona del VRAEM (2014 – 2016). Realizó acciones militares en apoyo a la PNP y la Fiscalía Especializada en materia ambiental en la lucha contra la minería ilegal en Madre de Dios. Ha realizado cursos de especialización sobre la gestión eficiente del presupuesto y el Sistema de abastecimiento y contrataciones publicas siendo certificado por el Organismo Supervisor de las Contrataciones del Estado (OSCE). Ha culminado la Maestría en Gestión Pública.*

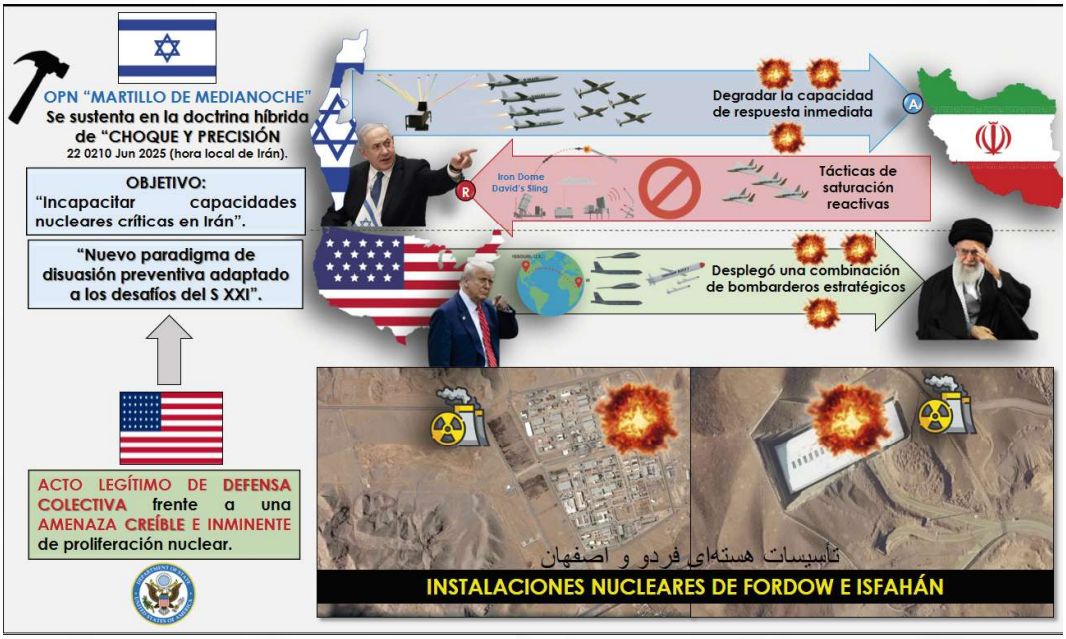
## 2. CONTEXTO GEOPOLÍTICO DEL CONFLICTO

El año 2025 estuvo atravesado por un deterioro sostenido de las relaciones entre Irán e Israel, alimentado por la ruptura definitiva del Plan de Acción Integral Conjunto (PAIC), cuya inestabilidad venía arrastrándose desde años atrás. La reactivación del programa nuclear iraní, acompañada del enriquecimiento de uranio a niveles superiores al 80% en las instalaciones de Fordow e Isfahán, generó una profunda inquietud a nivel internacional, especialmente en Washington y Tel Aviv, que interpretaron esta maniobra como un umbral técnico hacia la capacidad armamentística nuclear (The Sun, 2025).

En un intento de neutralizar anticipadamente esa amenaza, Israel lanzó una ofensiva encubierta de ciberataques contra los sistemas SCADA[1] que controlaban procesos industriales críticos en las principales instalaciones nucleares iraníes. Esta primera fase, carente de anuncios oficiales, pero de alto impacto operativo, estuvo orientada a degradar la capacidad de respuesta inmediata de Teherán, particularmente sus plataformas de defensa antiaérea (War on the Rocks, 2025).

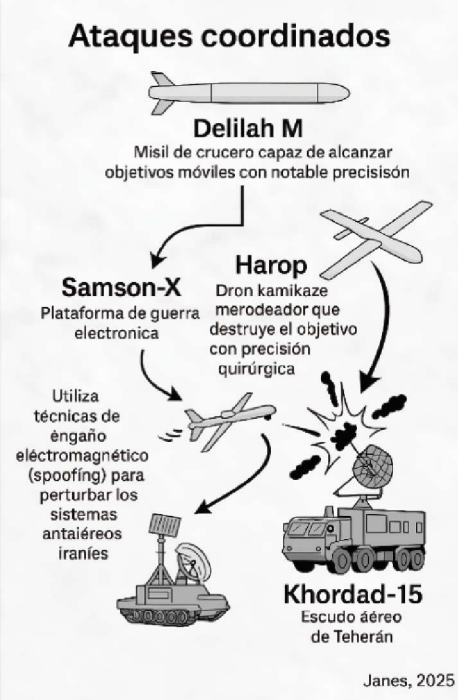
1 Los sistemas SCADA (Supervisory Control and Data Acquisition) son plataformas tecnológicas utilizadas para el control, supervisión y adquisición de datos en infraestructuras industriales complejas.

**FIGURA 1 CONTEXTO DEL CONFLICTO IRÁN - ISRAEL - EEUU.**




*Fuente: En base a la información publicada por The Sun y War on the Rocks (2025), imágenes asistidas por Copilot.*

**FIGURA 2 INFOGRAFÍA DE LA INTEGRACIÓN DE RECURSOS EN LOS ATAQUES COORDINADOS REALIZADOS POR LA FDI ISRAELÍ.**




*Nota: En base a la información publicada por Janes (2025) asistida por Copilot.*

El conflicto dejó rápidamente el plano cibernético y se trasladó al escenario cinético[2]. Irán respondió mediante un ataque masivo con misiles balísticos dirigidos contra bases militares israelíes y estadounidenses desplegadas en el Golfo Pérsico y en zonas de influencia en Siria e Irak.

La respuesta estadounidense no se hizo esperar: una contraofensiva aérea y naval fue desplegada de inmediato, inaugurando así un conflicto abierto de doce (12) días que alteró sustancialmente la correlación de fuerzas en Medio Oriente y puso en evidencia la velocidad con la que las guerras del siglo XXI pueden escalar de lo invisible a lo abiertamente devastador.

## 3. INNOVACIONES TECNOLÓGICAS EN COMBATE

Uno de los elementos más significativos del conflicto fue la sofisticada integración entre armamento convencional de alta precisión, operaciones de guerra electrónica (GE: WE) y estrategias de guerra cognitiva. Las Fuerzas de Defensa de Israel (FDI) ejecutaron ataques coordinados utilizando misiles

2 Un escenario cinético es un entorno de conflicto militar donde se emplea fuerza física o letal, mediante combate directo, fuego real y destrucción material. El término alude a la dimensión violenta y tangible de la guerra.

***Capitan EP***
***Abel Guzmán Lavado***

*Egresado de la Escuela Militar de Chorrillos "Francisco Bolognesi" como Subteniente del Arma de Infantería. Inició su carrera en el Batallón de Tanques "Crl. Carlos Llosa Llosa" N.° 223 en Tumbes. Prestó funciones en Cajamarca, Amazonas y Huancavelica. Formó parte de la BCT Huallhua del Batallón Contra Terroristas N.° 43 en Pampas–Tayacaja, participando en operaciones contra remanentes de Sendero Luminoso. Curso de Paracaidismo Militar y Curso Básico del Arma de Infantería, Diplomado en Gestión de Inversiones por la Universidad Científica del Sur. Actualmente se desempeña como Jefe del Departamento de Inversiones del Comando General de Apoyo del Ejército.*


100

de crucero Delilah M (capaces de alcanzar objetivos móviles con notable precisión) junto con drones kamikaze Harop, diseñados para merodear sobre el objetivo y destruirlo con precisión quirúrgica. Estos sistemas fueron respaldados por plataformas de GE (WE) Samson-X, que utilizaron técnicas de engaño electromagnético y spoofing para perturbar y neutralizar los sistemas antiaéreos iraníes, incluidos los Khordad-15, uno de los principales componentes del escudo aéreo de Teherán (Janes, 2025).

EE. UU. complementó estas acciones desde su base en Whiteman, Missouri, desplegando una combinación de bombarderos estratégicos B-2A Spirit y B-52H Stratofortress, ambos equipados con municiones penetrantes GBU-57A/B Massive Ordnance Penetrator (MOP), específicamente diseñadas para destruir instalaciones subterráneas profundamente fortificadas como las de Natanz y Fordow.

**FIGURA 3 INFOGRAFÍA DE LA INTEGRACIÓN DE RECURSOS EN LAS ACCIONES REALIZADAS POR EEUU.**


*Fuente: Esquema asistido por Copilot.*

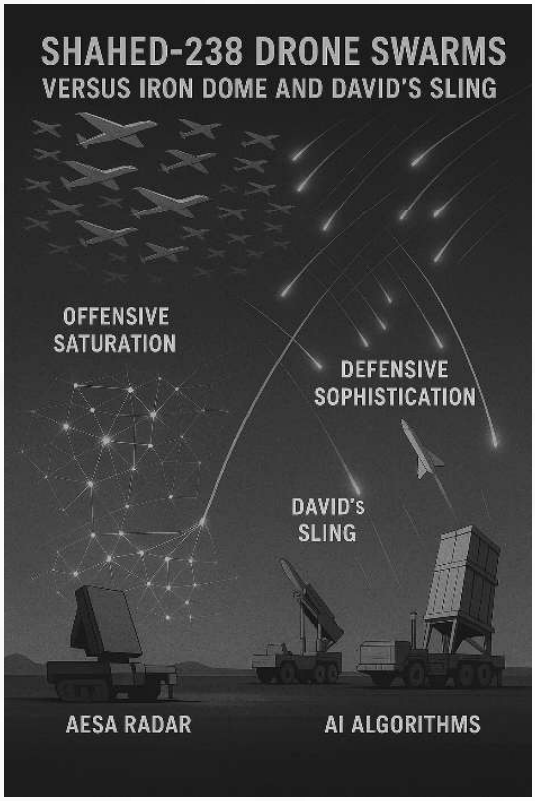
Además, se registró el empleo de misiles Tomahawk Block V (con capacidad de vuelo adaptativo, navegación asistida por inteligencia artificial y carga hiperbárica), lo que reveló un nivel avanzado de interoperabilidad entre sensores tácticos, sistemas de inteligencia en tiempo real y plataformas ofensivas (U.S. Naval Institute, 2025). En respuesta, Irán optó por tácticas de saturación mediante enjambres de drones Shahed-238, diseñados para desbordar los sistemas de defensa enemiga a través de ataques múltiples y simultáneos. Sin embargo, la eficacia de los sistemas de defensa aérea israelíes, como el Iron Dome y el David's Sling, quedó demostrada al interceptar la mayoría de estos dispositivos. Ambas plataformas integran radares AESA de escaneo electrónico activo y algoritmos de predicción cinemática potenciados por inteligencia artificial, lo cual permitió una respuesta ágil y automatizada ante la amenaza aérea (The Times of Israel, 2025).

## 4. ROL DE LA INTELIGENCIA ESTRATÉGICA Y CIBERNÉTICA

La inteligencia estratégica desempeñó un papel decisivo en el desarrollo del conflicto. En los días previos a las hostilidades abiertas, el Mossad, en coordinación con la Agencia de Seguridad Nacional de Estados Unidos (NSA), ejecutó una operación conjunta de intercepción de señales (SIGINT) y vigilancia electrónica avanzada. Esta colaboración permitió identificar y desarticular de forma anticipada nodos críticos del sistema iraní de mando y control, generando así una ventaja operativa que se tradujo en una respuesta inmediata y altamente coordinada desde el inicio del conflicto (Middle East Eye, 2025; The CyberWire, 2025).

Paralelamente, el control del espacio informacional se convirtió en un componente estratégico de primer orden. Mediante campañas de desinformación cuidadosamente diseñadas e impulsadas en redes sociales, Israel y EEUU lograron restringir la capacidad del régimen iraní para influir en la opinión pública internacional. Al mismo tiempo, construyeron una narrativa legitimadora que enmarcó las ofensivas como acciones defensivas, quirúrgicas y orientadas a neutralizar amenazas inminentes, lo que permitió reducir el costo político de las opera-

**FIGURA 4 INFOGRAFÍA DE LA INTEGRACIÓN DE RECURSOS EMPLEADOS POR IRÁN E ISRAEL RESPECTIVAMENTE.**




*Fuente: En base a la información publicada por la U.S. Naval Institute (2025), esquema asistido por Copilot.*

ciones en el plano diplomático (Council on Foreign Relations, 2025).

## 5. LA PARTICIPACIÓN ESTADOUNIDENSE: DOCTRINA, DISUASIÓN Y ACCIÓN DECISIVA

La intervención directa de EEUU en el conflicto, concretada mediante bombardeos de precisión sobre instalaciones estratégicas dentro del territorio iraní, se enmarcó en el acuerdo de cooperación bilateral en defensa que mantiene con Israel. No obstante, el aspecto más relevante de esta acción no fue su despliegue militar en sí, sino el giro doctrinario que implicó: por primera vez desde 2003, Washington abandonó su postura de contención pasiva frente a Teherán para adoptar una estrategia de disuasión activa y ofensiva (Reuters, 2025).

La operación, denominada "Martillo de Medianoche", se sustentó en una doctrina híbrida de "choque y precisión", orientada a proyectar fuerza letal con una presencia terrestre mínima. Según declaraciones del Gral Kenneth F. McKenzie Jr., excomandante del Comando Central de Estados Unidos (CENTCOM), el objetivo operativo no solo fue incapacitar capacidades nucleares críticas en sitios como Natanz y Fordow, sino también establecer "un nuevo paradigma de disuasión preventiva adaptado a los desafíos del siglo XXI" (Financial Times, 2025).

La respuesta institucional desde Washington fue inmediata y contundente. EEUU respaldó la operación como un acto legítimo de defensa colectiva frente a lo que consideró una amenaza creíble e inminente de proliferación nuclear en la región. En esa línea, el Departamento de Estado (DOS) emitió una declaración oficial advirtiendo que cualquier ataque contra personal o instalaciones estadounidenses sería interpretado como un casus belli con consecuencias regionales de amplio alcance (U.S. Department of State, 2025).

## 6. ENSAYO DE LA LECCIÓN APRENDIDA

El enfrentamiento trilateral entre Irán, Israel y EEUU, ocurrido en abril de 2025, constituye un caso paradigmático para el estudio de la evolución de la guerra en el siglo XXI. En un lapso inferior a 120 horas, se desplegaron capacidades militares de última generación con un nivel de letalidad e impacto estratégico sin precedentes, pero con una huella física mínima sobre el terreno. Irán lanzó misiles hipersónicos de alcance intermedio como parte de su capacidad de disuasión regional; Israel respondió mediante el uso de enjambres de drones kamikaze equipados con sistemas de navegación autónoma e inteligencia artificial, los cuales destruyeron plataformas de lanzamiento sin necesidad de una incursión terrestre. De forma simultánea, EEUU intervino desde la órbita baja terrestre utilizando armas de energía dirigida y pulsos electromagnéticos para inutilizar redes de mando y control iraníes (Defense One, 2025; Breaking Defense, 2025).

a. La lección central:

Durante gran parte de la segunda mitad del siglo XX, la doctrina de disuasión se construyó sobre la lógica de la demostración visible de poder: ejércitos

masivos, despliegues navales estratégicos, fuerzas nucleares en estado de alerta y ejercicios conjuntos diseñados para exhibir capacidades letales ante eventuales adversarios. Sin embargo, el conflicto de 2025 reveló que esa noción clásica ha sido superada por una forma de disuasión mucho más precisa, silenciosa y tecnológicamente sofisticada. Ya no se trata de intimidar con el número de divisiones blindadas o la presencia de un portaaviones, sino de integrar sensores orbitales, plataformas autónomas y sistemas de respuesta instantánea que convierten la vigilancia en letalidad sin previo aviso. Un ejemplo paradigmático lo constituyen los ataques preventivos basados en inteligencia satelital térmica, capaces de detectar el calentamiento de una rampa de lanzamiento iraní incluso antes del inicio de una operación, activando drones de ataque autónomos que neutralizan la amenaza en cuestión de segundos (Defense One, 2025). Este nuevo modelo de disuasión exige una revisión profunda de las doctrinas militares: si el diseño estratégico aún se mide en volumen de fuego o en fuerzas desplegadas, y no en velocidad de respuesta e interoperabilidad digital, se está preparando para conflictos del siglo pasado, no para los desafíos reales del entorno operativo actual.

b. Multi-dominio:

El conflicto entre Irán, Israel y EEUU evidenció que la guerra moderna ya no puede ser concebida como una operación unidimensional centrada en la supremacía de un único componente bélico. Por el contrario, se configuró como una acción simultánea y sincronizada en múltiples dominios operativos, en los que cada elemento cumplió un rol específico dentro de una arquitectura de combate interdependiente. Esta "sinfonía militar", como ha sido denominada por analistas del U.S. Joint Chiefs of Staff (2025), se libró sobre seis capas estratégicas articuladas con precisión.

El mensaje que deja esta experiencia es contundente: en el entorno bélico actual, la pérdida del control sobre un solo dominio puede fracturar la coherencia de la operación y traducirse en una derrota estratégica irreversible. En consecuencia, la formación militar actual no debe limitarse al dominio exclusivo de las tácticas especializadas, sino que debe incluir una comprensión integral de la lógica subyacente a la guerra multidominio, así como la ca-

**FIGURA 5 INFOGRAFÍA DE LAS OPERACIONES MULTIDOMINIO CONFIGURADAS Y DESPLEGADAS EN EL CONFLICTO IRÁN - ISRAEL - EEUU.**


*Fuente: En base a la información publicada por la U.S. Joint Chiefs of Staff (2025), imágenes asistidas por Copilot.*

pacidad de integrar de manera eficiente los medios tecnológicos avanzados con las capacidades operativas tradicionales.

c. Información:

Durante el conflicto, Irán no solo activó su capacidad misilística, sino que, en paralelo, desplegó una intensa campaña de desinformación a través de sus plataformas digitales oficiales y afines. Imágenes que mostraban la supuesta destrucción de infraestructuras civiles por parte de Israel fueron difundidas con rapidez, buscando impactar emocionalmente a la opinión pública internacional y desacreditar la legitimidad de la operación aliada.

Sin embargo, la respuesta técnico-informativa no se hizo esperar: en menos de quince (15) minutos, unidades especializadas de ciberinteligencia analizaron los metadatos de los archivos, los cruzaron con datos de geolocalización y demostraron que el proyectil provenía de un lanzador ubicado en las afueras de Teherán (Center for Strategic and International Studies [CSIS], 2025). La disputa narrativa, en este caso, fue resuelta antes de que los medios de comunicación pudieran desplegarse en el terreno.

Este episodio evidencia que el control del relato se ha convertido en un componente estratégico de las operaciones modernas. La información, en contextos de alta intensidad bélica, no es un simple complemento: es un vector operacional que puede reforzar o comprometer la legitimidad del uso de la fuerza. Comunicar sin verificar los datos o sin respetar los protocolos establecidos no solo pone en riesgo la credibilidad institucional, sino que puede traducirse en pérdidas operativas tangibles. Por ello, se vuelve imperativo que el personal militar integre, como parte de su formación profesional, el manejo ético, técnico y oportuno de la información, al mismo nivel de exigencia que la ejecución táctica en el campo.

d. Velocidad de decisión:

Durante el conflicto, el tiempo transcurrido entre la detección de un objetivo y su neutralización alcanzó un nivel sin precedentes: apenas 3 minutos con 42 segundos. Esta eficiencia operativa fue posible gracias a una arquitectura de mando descentralizado (basada en la figura del "mando delegado") y al empleo de algoritmos de priorización que permitieron seleccionar blancos en tiempo real sin necesidad de escalar cada decisión a niveles superiores.

Esta autonomía táctica, respaldada por inteligencia artificial y protocolos previamente definidos, resultó clave para preservar la velocidad y la letalidad del esfuerzo conjunto. En contraposición, la respuesta iraní a los ataques iniciales se vio demorada por más de 2 horas, debido a cuellos de botella en la autorización jerárquica, lo que redujo considerablemente su eficacia operativa (Defense Innovation Unit, 2025; RAND Corporation, 2025).

La lección derivada es clara: la lentitud en la toma de decisiones no es una consecuencia inevitable de los sistemas democráticos, siempre que las reglas de enfrentamiento, las líneas de autoridad y los criterios éticos estén definidos de forma anticipada y sean interiorizados por quienes deben actuar sobre el terreno. Desde esta perspectiva, resulta esencial entender la autonomía táctica no como un derecho, sino como una responsabilidad que requiere una sólida formación, juicio operativo y un fundamento ético consistente. Únicamente bajo estos principios podrá ejercerse un mando ágil y legítimo en entornos donde la temporalidad es un factor crítico para el cumplimiento de la misión.

e. Ética y proporcionalidad:

Durante los primeros días del conflicto, un dron autónomo equipado con inteligencia artificial ejecutó con éxito una operación de precisión contra un alto mando iraní que se desplazaba en un vehículo blindado. El sistema, tras analizar múltiples variables tácticas y ambientales, determinó que el ataque implicaba una probabilidad nula de víctimas colaterales. Sin embargo, días después, un dron similar erró su objetivo y destruyó un autobús escolar, provocando una tragedia humanitaria que eclipsó por completo el precedente operativo exitoso. El episodio puso en evidencia un fenómeno recurrente en la guerra moderna: mientras la tecnología incrementa la precisión táctica, también amplifica la exposición política, legal y ética de cada decisión automatizada (International

Committee of the Red Cross [ICRC], 2025; Human Rights Watch, 2025). La principal enseñanza es ineludible, el desarrollo de sistemas de combate autónomos no puede avanzar desligado de la normatividad internacional vigente. Tan urgente como calibrar sensores ópticos o refinar algoritmos de navegación, es integrar desde la arquitectura del firmware los principios del Derecho Internacional Humanitario (DIH). En el entorno operacional contemporáneo, el uso de inteligencia artificial no solo debe ser eficaz, sino legítimo. Por ello, el profesional militar del siglo XXI está llamado a comprender que la responsabilidad sobre el uso de la fuerza no puede delegarse por completo en un código: debe ser acompañada por supervisión humana, criterios éticos claros y estrictos protocolos de empleo operacional.

f. Interoperabilidad:

Durante la operación, cada piloto israelí contó con acceso directo a canales criptográficos de la Fuerza Aérea de los Estados Unidos (USAF), lo que permitió una coordinación segura y sin interferencias en tiempo real. Al mismo tiempo, los analistas de la Agencia de Seguridad Nacional (NSA) recibían directamente los flujos de datos recopilados por los drones Hermes 900, sin necesidad de realizar procesos de conversión entre sistemas.

Este nivel de interoperabilidad avanzada no fue producto de una respuesta improvisada, sino el resultado de más de una década de ejercicios bilaterales, desarrollo conjunto de protocolos operacionales y la consolidación de una doctrina de combate común entre ambos países (U.S. Department of Defense, 2025; Israeli Ministry of Defense, 2025).

La principal enseñanza es clara: la interoperabilidad real no se alcanza únicamente mediante la adquisición de plataformas compatibles en términos tecnológicos. Para operar eficazmente en escenarios de alta exigencia táctica, es indispensable establecer doctrinas compartidas, entrenar bajo entornos multinacionales realistas y construir confianza operativa antes de que surja una crisis. En este contexto, la integración doctrinal previa se convierte en un factor crítico para garantizar una respuesta conjunta efectiva y oportuna frente a amenazas complejas.

g. Inteligencia:

Una proporción significativa de los misiles iraníes nunca alcanzó a despegar durante el conflicto, debido a un sistema de detección anticipada altamente integrado. La secuencia comenzó con sensores infrarrojos satelitales que identificaron patrones térmicos anómalos en rampas de lanzamiento; estos datos fueron validados mediante interceptación de señales electrónicas (SIGINT), y concluyó con su neutralización inmediata por vehículos aéreos no tripulados (UAV), guiados por actualizaciones tácticas en tiempo real desde centros de comando conjunto (National Reconnaissance Office, 2025; NATO CCDCOE, 2025).

Este episodio ilustra con claridad que la inteligencia ya no es una herramienta reservada exclusivamente para los altos mandos estratégicos, sino un insumo operacional de uso cotidiano en todos los niveles del combate. En el entorno de guerra multidominio, la información procesada con precisión y velocidad se ha convertido en la primera "munición" que se activa, incluso antes que cualquier armamento físico. Por tanto, formar al personal militar para recolectar, interpretar y actuar sobre datos de inteligencia debe ser una prioridad institucional equivalente (o incluso superior) a su entrenamiento convencional con sistemas de armas. La destreza técnica debe ir acompañada por una capacidad analítica que permita tomar decisiones en tiempo real, con responsabilidad táctica y comprensión del entorno operativo digital.

h. Profesionalización:

La breve, pero decisiva guerra de 2025 fue ganada por aquellos que, desde 2022, ya se entrenaban en escenarios de alta complejidad: simuladores de guerra cognitiva, cursos especializados en ética aplicada a la inteligencia artificial, y ejercicios binacionales con aliados estratégicos. Esta experiencia evidenció que la profesión militar debe transformarse de un enfoque centrado exclusivamente en la capacidad de destrucción (el “especialista en letalidad”) hacia un nuevo paradigma: el del gestor del poder regulado, un profesional capaz de integrar tecnologías disruptivas, marcos jurídicos internacionales y comprensión del comportamiento humano

en contextos operativos impredecibles (Center for a New American Security, 2025; NATO ACT, 2025).

Este giro conceptual exige una reforma profunda de los modelos de formación y desarrollo de carrera dentro de las instituciones castrenses. En concreto, se requieren tres (03) transformaciones clave:

- Currículos interdisciplinares, que combinen ingeniería de sistemas, derecho operacional y ciencias cognitivas, preparando al personal para tomar decisiones complejas bajo presión moral y tecnológica.
- Centros de entrenamiento multifuncionales, que incorporen entornos simulados de desinformación, manipulación narrativa y guerra informativa como parte integral de los polígonos de instrucción.
- Sistemas de promoción basados en mérito adaptativo, donde se valoren la capacidad de innovación, juicio ético y pensamiento crítico por encima de la antigüedad estricta o la permanencia en el servicio.

Esta transformación no es opcional ni teórica: constituye una condición de viabilidad para mantener tanto la eficacia operativa como la legitimidad política de la acción militar en escenarios cada vez más multidominio, autónomos y expuestos al escrutinio público global.

## EPÍLOGO:

### 1. La guerra de quinta generación (5 WoG): un nuevo paradigma operativo

El conflicto entre Irán, Israel y EEUU en 2025 marcó el inicio de una nueva era en la evolución de la guerra contemporánea: la guerra de quinta generación (5WoG). Este entorno operativo se define por la fusión entre lo militar y lo civil, lo físico y lo digital, donde los campos de batalla no se limitan a coordenadas geográficas, sino que se extienden al control de la información, a la manipulación de la percepción y al uso inteligente de tecnologías emergentes.

En este marco, la superioridad estratégica ya no depende únicamente del poder de fuego o del número de efectivos, sino de la agilidad institucional y de la capacidad cognitiva de los actores involucrados para anticipar, integrar y reaccionar en tiempo real.

Como señalan Schmidt & Cohen (2025) y el NATO Innovation Hub (2025), esta transformación exige un replanteamiento profundo de las doctrinas tradicionales, alineándolas con una realidad donde la velocidad, la interoperabilidad y la inteligencia informan cada acción táctica.

### 2. Gestión de combate: el eje de la guerra del siglo XXI

Este nuevo escenario redefine el concepto de "Gestión de Combate" (Combat Management – CM), entendido como la capacidad de planificar, coordinar y ejecutar operaciones mediante una integración ágil de recursos humanos, tecnológicos y organizacionales bajo condiciones de presión y alta incertidumbre.

Más allá del mando y control tradicional, la gestión de combate se convierte en una disciplina que integra una toma de decisiones rápidas, informada y éticamente fundamentada, donde la temporalidad emerge como un recurso estratégico esencial: el ritmo operativo, la sincronización entre dominios y la anticipación de efectos definen el éxito táctico y la iniciativa estratégica.

La experiencia del conflicto de 2025 demuestra que la guerra contemporánea no se gana únicamente con armamento avanzado, sino con sistemas interoperables, inteligencia en tiempo real y líderes capacitados para decidir bajo presión. En este contexto, la gestión de combate se posiciona como el eje articulador entre doctrina, tecnología y ética operativa, donde quien administra con precisión el tiempo y los recursos obtendrá la ventaja decisiva.

Por ello, formar al personal militar bajo paradigmas obsoletos equivale a prepararlo para conflictos del pasado; la verdadera exigencia estratégica del siglo XXI es desarrollar capacidades institucionales y humanas que aprenden, adaptan y actúan más rápido que el adversario, en un entorno donde el cambio es permanente y la incertidumbre, estructural.

**TABLA 1 MATRIZ DE INNOVACIONES DEL CONFLICTO IRÁN-ISRAEL-EEUU 2025.**

| Dominio | Innovación | Dispositivo / Sistema | Doctrina Habilitada | Lección aprendida | Riesgo Ético / Legal |
|---|---|---|---|---|---|
| Espacial | Satélites IR[3] de última generación | SBIRS-GEO 3 | Detección de calor pre-lanzamiento (ventana 3'42'') | "Inteligencia es la primera munición" | Sobrevuelo sin consentimiento |
| Cibernético | Spoofing[4] de radares Khordad-15 | Samson-X EW | Guerra electromagnética ofensiva[5] | Integrar EW en ciclo F2T2EA[6] | Posible daño colateral a redes civiles |
| Aéreo | Enjambre de drones kamikaze | Harop | Saturación + selección autónoma | Delegar decisión a IA, pero con human-on-the-loop[7] | Responsabilidad por algoritmo |
| Terrestre | Fuerzas especiales "pintoras"[8] | Unit 669 | Marca láser + bombardeo hipersónico | Trabajo interdependiente con aviación | Identificación errónea de blancos |
| Marítimo | Submarinos con Tomahawk V | USS Georgia | Hostigamiento de líneas de abastecimiento | Ocultar fuerza hasta el momento decisivo | Violaciones de aguas territoriales |
| Cognitivo | Campaña de desinformación anticipada[9] | NSA/NGA | Narrativa que precede al proyectil | Comunicar antes que el adversario | Manipulación de opinión pública |
| Ético | IA con filtro de Derecho Internacional[10] | Ethics Chip | Proporcionalidad en microsegundos | Programar leyes de guerra en firmware[11] | Fallo algorítmico → caso: autobús escolar |
| Interoperabilidad | Radio criptográfica bilateral | LINK-16 LATAM | Mando delegado USA-Israel | Entrenar doctrinas comunes antes del conflicto | Brecha si aliado no actualiza firmware |

3 Es un observatorio espacial de altísima resolución térmica que capta la radiación infrarroja (IR) emitida por la superficie o por objetos en movimiento, día y noche, sin depender de la luz solar.

4 Spoofing es una técnica de GE (EW) que consiste en engañar a un sistema de detección o navegación haciéndole creer que está recibiendo señales legítimas cuando en realidad son falsas, manipuladas o retransmitidas por un atacante.

5 Offensive electromagnetic warfare (OEW) es el conjunto de acciones militares activas (AMO) que, valiéndose del espectro electromagnético o de energía dirigida, buscan atacar, degradar, engañar o destruir los sistemas electrónicos del adversario para negarle su ventaja y garantizar la libertad de acción propia.

6 Integrar EW en el ciclo F2T2EA significa insertar la GE (EW) como una capa transversal y activa, de modo que el ataque o la defensa no dependan solo de sensores y armas cinéticas, sino también de la capacidad para dominar o degradar el espectro electromagnético en tiempo real.

7 Consiste en permitir que la IA seleccione y ejecute acciones militares de manera autónoma, pero siempre bajo la supervisión activa humana que pueda intervenir, corregir o cancelar cualquier decisión en tiempo real.

8 Este concepto proviene de la doctrina "láser-designation & stand-off strike" empleada por Unit 669 (fuerzas de combate israelíes) y Navy SEALs estadounidenses, donde la misión crítica es marcar (pintar) silos, plataformas de lanzamiento o búnkeres nucleares y retirarse antes de que lleguen los proyectiles hiperbálicos o enjambres de drones kamikaze.

9 Se trata de una operación de información ofensiva lanzada antes de que ocurra el primer disparo (o incluso antes de que se tome una decisión pública). Su objetivo es pre-colorear la percepción global sobre quién es el agresor, qué está en juego y cuál es la "respuesta legítima".

10 IA con filtro de Derecho Internacional nos referimos a un sistema de inteligencia artificial que, antes de ejecutar una acción letal o de alto impacto, consulta y aplica en tiempo real las normas del DIH, los DDHH y los principios de proporcionalidad/distinción.

11 Traducir el DIH a código para que el arma no dispare si violaría la legalidad, manteniendo siempre responsabilidad humana final.

## REFERENCIAS

Al Jazeera. (2025, julio 15). Israel-Iran conflict enters 12th day as US backs precision strikes. Al Jazeera. https://www.aljazeera.com/news/2025/7/15/israel-iran-conflict-enters-12th-day-as-us-backs-precision-strikes

Breaking Defense. (2025, julio 18). US Space Command details EMP strikes on Iranian C2 networks. https://breakingdefense.com/2025/07/us-space-command-details-emp-strikes-on-iranian-c2-networks

Center for Strategic and International Studies. (2025). Iran-Israel 2025: Lessons in multi-domain warfare. CSIS Briefs. https://www.csis.org/analysis/iran-israel-2025-lessons-multi-domain-warfare

Centro de Innovación de la OTAN. (2025). Campos de batalla del futuro: Dominios emergentes en la guerra de quinta generación. Organización del Tratado del Atlántico Norte. https://www.nato.int/innovation-hub/2025

Centro para una Nueva Seguridad Estadounidense. (2025). Educación militar para el siglo XXI: Reformando el entrenamiento y la doctrina para la guerra multidominio. https://www.cnas.org/publications/2025

Comando Central de EE. UU. (CENTCOM). (2025). Operación Martillo de Medianoche: Informe táctico y estrategia de disuasión activa [Informe no publicado]. CENTCOM.

Council on Foreign Relations. (2025, julio 20). Narrative dominance: Disinformation campaigns in the 2025 Middle East conflict. CFR Backgrounders. https://www.cfr.org/backgrounder/narrative-dominance-disinformation-campaigns-2025

Defense Innovation Unit. (2025). Speed of decision: Delegated authority in Martillo de Medianoche (Report DIU-2025-07). U.S. Department of Defense. https://www.diu.mil/library/reports/2025/diu-2025-07

Defense One. (2025, julio 17). Inside the 3-minute kill chain: AI, heat signatures, and human override. https://www.defenseone.com/threats/2025/07/inside-3-minute-kill-chain-ai-heat-signatures-and-human-override/391784

El País. (2025). EE. UU., Reino Unido, Francia y Alemania dan un ultimátum a Irán para firmar un acuerdo nuclear antes de septiembre. https://elpais.com/internacional/2025-07-16

Estado Mayor Conjunto (EE.UU.). (2025). Informe sobre operaciones multidominio en el conflicto Irán-Israel-EEUU [Informe estratégico]. Ministerio de defensa.

Financial Times. (2025, julio 19). McKenzie: "A new paradigm of preventive deterrence". https://www.ft.com/content/d1ca58cb-7243-4fd1-803e-de4ee61a36fd

Human Rights Watch. (2025). Algorithmic warfare and civilian harm: The 2025 Iran-Israel case study (HRW Report). https://www.hrw.org/report/2025/07/22/algorithmic-warfare-civilian-harm

International Committee of the Red Cross. (2025). Autonomy in weapon systems: Legal and ethical implications (ICRC Position Paper). https://www.icrc.org/en/document/autonomy-weapon-systems-2025

Israeli Ministry of Defense. (2025, julio 21). IDF-Hermes 900 integration with USAF data links (Press Release). https://www.gov.il/en/departments/news/idf-hermes900-usaf-2025

Janes Defence Intelligence. (2025). Delilah M, Harop and Samson-X: EW triad in the 2025 Iran-Israel War. Janes. https://www.janes.com/defence-news/iran-israel-2025-ew-triad

Middle East Eye. (2025, julio 15). Mossad-NSA SIGINT blitz pre-empted Iranian command nodes. https://www.middleeasteye.net/news/mossad-nsa-sIGINT-blitz-2025

National Reconnaissance Office. (2025). Thermal-satellite early-warning in Operation Martillo de Medianoche (NRO Fact Sheet). https://www.nro.gov/news/2025/martillo-thermal-early-warning

NATO ACT. (2025). Future military professional: interdisciplinary curriculum recommendations. https://www.act.nato.int/publications/future-military-professional-2025

NATO CCDCOE. (2025). Cyber lessons from the 2025 Middle East crisis (CCDCOE Report). https://ccdcoe.org/publications/2025-cyber-lessons-middle-east

Reuters. (2025, julio 16). Iran ready to respond to any new attack, supreme leader says. https://www.reuters.com/world/middle-east/iran-re-

ady-respond-any-new-attack-supreme-leader-says-2025-07-16

RAND Corporation. (2025). Delegated authority and decision speed in high-tempo operations: 2025 case study. RAND Perspectives. https://www.rand.org/pubs/perspectives/PEA2580-1.html

Schmidt, E., & Cohen, J. (2025). The next battlefield: AI, autonomy and the future of war. Penguin Press.

The CyberWire. (2025, julio 18). SIGINT and cyber pre-emption: The Mossad-NSA playbook. https://thecyberwire.com/stories/2025/07/18/sigint-cyber-preemption

The Jerusalem Post. (2025, julio 14). Twelve days that changed the Middle East: Inside the 2025 war. https://www.jpost.com/middle-east/12-days-that-changed-the-middle-east-2025

The Sun. (2025, julio 15). Iran boosts uranium enrichment as Fordow bombed. https://www.thesun.ie/news/15551099/iran-uranium-enrichment-nuclear-fordow-strikes

The Times of Israel. (2025, julio 16). Iron Dome, David's Sling intercept 97 % of Iranian drones. https://www.timesofisrael.com/iron-dome-davids-sling-intercept-97-percent-iranian-drones

U.S. Department of Defense. (2025). Joint doctrine note 1-25: Multi-domain operations in the 2025 Middle East conflict. https://www.defense.gov/publications/jdn-1-25

U.S. Department of State. (2025, julio 18). Statement on casus belli threshold in the 2025 Iran conflict. https://www.state.gov/2025-iran-casus-belli-statement

U.S. Naval Institute. (2025). Tomahawk Block V: Precision, AI and the 2025 strikes. Proceedings Magazine, 151(7), 34-41. https://www.usni.org/magazines/proceedings/2025/july/tomahawk-block-v

War on the Rocks. (2025, julio 20). Cyber, missiles and drones: Lessons from the Israel-Iran war. https://warontherocks.com/2025/07/cyber-missiles-drones-israel-iran

Wikipedia (2025). Ataques de Estados Unidos contra Irán de 2025. https://es.wikipedia.org/wiki/Ataques_de_Estados_Unidos_contra_Ir%C3%A1n_de_2025