

XXVII CONFERENCIA DE DIRECTORES DE
COLEGIOS DE DEFENSA IBEROAMERICANOS

LA INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS EN LOS ESCENARIOS DE OPERACIONES FUTUROS

LA INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS
EN LOS ESCENARIOS DE OPERACIONES FUTUROS



TOMO XV DEL LIBRO DE LA ACDIA PRESENTADA
EN LA XXVII CDCDIA CESEDEN ESPAÑA 2026



Dirección y coordinación

Director del Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

TG. Miguel Ballenilla y García de Gamarra

Director del Departamento de Cultura y Diplomacia de Defensa (DCDD) del CESEDEN

GB. Luis Carlos Torcal Ortega

Coordinador Académico y Secretario de Coordinación Permanente del CESEDEN ante ACDIA

Cor. Pedro Polo Campo

Revisores

Cor. Pedro Polo Campo

Cte. José Manuel Sánchez García

Cap. Alfonso Méndiz Guerra

© Autores y editor, 2026

Fecha de edición: junio 2026

Maqueta e imprime: Safekat

Las opiniones emitidas en esta publicación son exclusiva responsabilidad de los autores 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 100 % libre de cloro procedente de bosques gestionados de forma sostenible.



NOTA AL LECTOR

El Centro Superior de Estudios de la Defensa Nacional (CESEDEN), informa que realizó la compilación de los artículos para el tomo XV del libro de la Asociación de Colegios de Defensa Iberoamericanos (ACDIA) presentado en forma física en la XXVII Conferencia de Directores de Colegios de Defensa de Iberoamérica (CDCDIA) CESEDEN, España.

Se considera necesario subrayar que la responsabilidad de las afirmaciones y opiniones de los artículos recae exclusivamente en los autores y no expresan necesariamente el pensamiento del CESEDEN.

Es importante destacar que, por el respeto a la integridad intelectual de cada participante, se ha mantenido el contenido, unificando solamente la estructura y formato de los artículos conforme a las normas editoriales o los lineamientos establecidos para la elaboración de esta publicación.

Queda prohibida la reproducción parcial o total de la misma a través de cualquier medio sin previa autorización del CESEDEN, titular de todos los derechos.



ÍNDICE

- 19 **PRÓLOGO**
Miguel Ballenilla y García de Gamarra
- 25 **CAPÍTULO PRIMERO. BRASIL, ESCOLA SUPERIOR DE GUERRA (ESG)
LAS NUEVAS TECNOLOGÍAS Y EL FUTURO DE LA GUERRA**
Ricardo Rodrigues Freire
- 26 Aspectos introductorios
27 Descodificación de la guerra
31 *Las principales tecnologías que despuntan en el escenario de las guerras*
37 Implicaciones de las nuevas tecnologías para el futuro de la guerra
40 Conclusiones
43 Referencias
- 47 **CAPÍTULO SEGUNDO. BRASIL, ESCOLA SUPERIOR DE DEFESA
COMPETÊNCIAS E PRODUÇÃO DO CONHECIMENTO NO CAMPO DOS
ESTUDOS DE DEFESA: A INTELIGÊNCIA ARTIFICIAL GENERATIVA
COMO PARADIGMA EDUCATIVO**
Patrícia Pontes Bezerra
Aline Barbosa Xavier Muniz
Eduardo Amadeu Dutra Moresi
- 48 Introdução
49 Competências docentes: o papel da Escola Superior de Defesa nos Estudos de Defesa
55 Inteligência artificial generativa como paradigma educativo
57 *As teorias pedagógicas: TPACK*

58	<i>IAGen como objeto, meio e ambiente de formação</i>
59	Metodologia da pesquisa na base Scopus
65	<i>Resultados da pesquisa</i>
66	IA educacional, inovação pedagógica e aprendizagem personalizada
67	Competências docentes, ChatGPT, literacia em IA e TPACK
68	Educação militar, formação de instrutores e produção do conhecimento em Defesa
69	IA, segurança, guerra, estratégia e governança tecnológica
69	Segurança técnica de sistemas de IA, ciberdefesa e defesa algorítmica
70	Principais achados das categorias temáticas
72	Conclusão
74	Referências
81	CAPÍTULO TERCERO. COLOMBIA, ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”. DEFENSA MULTIDOMINIO: EVOLUCIÓN DE LOS SISTEMAS DE DEFENSA MULTICAPA EN LOS ESCENARIOS OPERACIONALES FUTUROS
	Fabio Leonardo Caro Cancelado
	Aldemar Serrano Cuervo
	Jonnathan Jimenez-Reina
82	Introducción
87	Sistemas de defensa multicapa: bases conceptuales y evolución inicial
90	Transformación del entorno estratégico y de las amenazas
94	<i>Límites del modelo clásico de defensa antiaérea</i>
98	De la defensa antiaérea a la defensa multidominio
101	Componentes de la evolución del sistema multicapa
105	Implicaciones estratégicas, operacionales y doctrinales
108	Conclusiones
111	Referencias

**119 CAPITULO CUARTO. ECUADOR, ACADEMIA DE DEFENSA MILITAR
CONJUNTA (ADEMIC). LA INFLUENCIA DE LAS NUEVAS
TECNOLOGÍAS EN LOS ESCENARIOS DE OPERACIONES FRENTE A
LAS AMENAZAS HÍBRIDAS Y CRIMEN ORGANIZADO
TRANSNACIONAL: UNA PERSPECTIVA**

Luis Fernando Pillajo

- 120 Introducción
- 121 Marco teórico
 - 121 *Estrategia y multidimensionalidad del conflicto*
 - 124 *Seguridad integral y amenazas contemporáneas*
 - 125 *Dominio de la información y guerra cognitiva*
- 127 Metodología
- 128 Resultados y discusión
 - 128 *Transformación de los escenarios operacionales*
 - 131 *Impacto en amenazas híbridas*
 - 131 *Crimen organizado transnacional*
- 133 Conclusiones
- 134 Referencias

**137 CAPÍTULO QUINTO. EL SALVADOR. COLEGIO DE ALTOS ESTUDIOS
ESTRATÉGICOS. INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS EN
LOS ESCENARIOS DE OPERACIONES FUTURAS**

Francisco Yohalmo de Jesús Mejía Martínez

- 138 Introducción
- 142 Operaciones Multidominio y su impacto con la tecnología
- 145 Actores Geoestratégicos, sus operaciones multidominio y sus avances tecnológicos en el siglo XXI: China – EE.UU. – Rusia
- 148 Factores que determinaron el grado de derrota relativa entre la alianza de EE.UU. e Israel contra Irán: ¿Tecnología, liderazgo, estrategia?
- 152 Conclusiones
- 153 Referencias

155 CAPITULO SEXTO. ESPAÑA, CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (CESEDEN). EL EMPLEO MILITAR DE LA INTELIGENCIA ARTIFICIAL

Carlos Javier Frías Sánchez

- 156 Introducción
- 157 La IA y sus usos militares
- 166 “Kill chains” y “kill webs”
- 170 Conclusiones
- 171 Bibliografía

173 CAPITULO SÉPTIMO. HONDURAS, COLEGIO DE DEFENSA NACIONAL. LA INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS EN LOS ESCENARIOS FUTUROS

Adán Antonio Ramírez Salinas

Nery Obdulio Mejía Espinoza

Rafael Antonio Maradiaga Molina

- 174 Introducción
- 175 Principales riesgos geopolíticos hasta 2026
- 178 La infraestructura crítica está en riesgo crítico
 - 178 *El impacto de las condiciones climáticas extremas*
 - 179 *La digitalización*
 - 179 *La silenciosa crisis de infraestructuras*
 - 180 *La necesidad de una visión holística*
 - 181 *Evolución de las TIC en los sistemas de defensa*
 - 183 *Mando y control militar con apoyo de TIC*
 - 186 *Ciberseguridad y defensa cibernética*
 - 188 *Interoperabilidad, integración y transformación digital*
 - 189 *Infraestructura crítica*
 - 190 *Ataques contra la infraestructura crítica*
 - 190 *Organización para la infraestructura crítica*
 - 191 *Protección de la infraestructura crítica*
 - 192 *Planificación sectorial de la infraestructura crítica*
 - 193 *Confidencialidad de la información de la infraestructura crítica*
 - 193 *Actores según sector*
 - 195 *Infraestructura crítica, brecha digital y capacidades del Estado*
- 199 Ética, legislación y soberanía digital en el uso de TIC para la seguridad nacional

199	<i>Ética y derechos fundamentales</i>
200	Conclusiones
201	Bibliografía
203	CAPÍTULO OCTAVO. MÉXICO, CENTRO DE ESTUDIOS SUPERIORES NAVALES (CESNAV). TECNOLOGÍAS DISRUPTIVAS Y SU IMPACTO EN LA SEGURIDAD GLOBAL DE LOS ESTADOS: UN NUEVO PARADIGMA
	David Sánchez Hernández (Ph.)
	Francisco Chávez Gutiérrez (Ph.)
205	Introducción
207	Transformación tecnológica y cambio del entorno estratégico global
209	Principales tecnologías disruptivas con impacto en la seguridad nacional
209	<i>Inteligencia artificial y aprendizaje automático</i>
210	<i>Ciberseguridad, ciberdefensa y guerra cognitiva</i>
210	<i>Drones, sistemas autónomos y plataformas no tripuladas</i>
211	<i>Computación cuántica y criptografía poscuántica</i>
212	<i>Biotecnología, bioseguridad y riesgos epidemiológicos</i>
213	<i>Tecnologías espaciales, satélites y vigilancia estratégica</i>
214	<i>Robótica militar y sistemas autónomos letales</i>
215	<i>Big data, vigilancia digital y análisis predictivo</i>
216	<i>Semiconductores, cadenas de suministro críticas y dependencia tecnológica</i>
216	<i>Energías avanzadas, materiales estratégicos y tecnologías duales</i>
218	<i>Tecnologías disruptivas y el futuro de las operaciones militares</i>
219	Implicaciones para la seguridad nacional
220	<i>Dimensión política</i>
220	<i>Dimensión económica</i>
220	<i>La dimensión social</i>
221	<i>La dimensión militar</i>
221	<i>La dimensión tecnológica</i>
222	<i>La dimensión diplomática</i>
222	<i>La dimensión ambiental</i>
223	<i>Riesgos estratégicos emergentes</i>
225	Oportunidades estratégicas para los Estados
226	Perspectiva para México e Iberoamérica
228	Escenarios prospectivos

228	<i>Escenario tendencial: adaptación desigual hacia 2035</i>
228	<i>Escenarios de riesgo: escalada tecnológica y fragmentación hacia 2035</i>
229	<i>Escenario ideal: soberanía tecnología y gobernanza responsable hacia 2035</i>
229	Conclusión
230	Recomendación estratégica
233	Referencias

235 CAPÍTULO NOVENO. MÉXICO, COLEGIO DE DEFENSA NACIONAL (CODENAL). ESCENARIOS FUTUROS DE LAS OPERACIONES MILITARES EN IBEROAMÉRICA

Edgar Ortiz Arellano

236	Introducción
237	Contexto actual
243	Visualización estratégica
245	Escenarios con Ejes de Schwartz
246	Escenario cuadrante I. "Fortaleza con innovación limitada"
247	Escenario cuadrante II. "Transformación operacional plena"
248	Escenario cuadrante III. "Modernización asimétrica"
249	Escenario cuadrante IV. "Inercia y rezago operacional"
250	Hacia escenarios disruptivos
250	Escenario disruptivo "Salto inesperado"
251	Escenario disruptivo "Tecnología sin control"
251	Incertidumbres
252	Recomendaciones
253	Conclusiones
254	Referencias

257 CAPÍTULO DECIMO. PARAGUAY. INSTITUTO DE ALTOS ESTUDIOS ESTRATÉGICOS (IAEE). LA INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS EN LOS ESCENARIOS DE OPERACIONES FUTUROS

Edwin Ramon Martínez González

Pedro Antonio Arguello Benitez

Héctor Antonio Aguirre
Carlos Alberto Martínez Galeano
Ruth Margarita Vallejos Espínola

259	Introducción
260	Evolución de la tecnología en los conflictos modernos
260	Del campo físico al entorno multidominio
263	Nuevas Tecnologías Disruptivas
272	Riesgos y Amenazas Futuras
272	<i>Dependencia tecnológica</i>
272	<i>Vulnerabilidades de IA</i>
272	<i>Deepfakes y desinformación</i>
273	<i>Ataques a infraestructuras críticas</i>
274	Impacto Estratégico Nacional
274	<i>Necesidad de capacidades nacionales de ciberdefensa</i>
274	<i>Formación de talento especializado</i>
275	<i>Cooperación internacional</i>
275	<i>Desarrollo doctrinario y normativo</i>
276	<i>La necesidad de integrar tecnología, doctrina y factor humano</i>
276	<i>La Prospectiva Estratégica</i>
277	<i>Arquitecturas Tecnológicas y Procesamiento Multidominio</i>
277	<i>Interoperabilidad de Sistemas de Armas y Datos: El Modelo de Mando y Control</i>
278	<i>El Factor Humano y la Dimensión Cognitiva en el Procesamiento del Mensaje</i>
279	<i>El Desafío de la Interoperabilidad Concurrente y la Fusión de Datos</i>
280	<i>Mitigación de la Interferencias y Protección del Receptor Humano</i>
280	<i>Horizonte a Largo Plazo: La Disrupción de la Guerra Algorítmica Generalizada y el Combate Autónomo</i>
281	<i>La Velocidad del Software como Vector Estratégico</i>
281	<i>Panorama General de la Transformación Tecnológica y la Revolución en los Asuntos Militares (RAM)</i>
282	<i>Desafíos Estratégicos, Éticos y de Estabilidad del Entorno Tecnológico</i>
283	<i>Operaciones en Entorno Multidominio y Ventaja Decisional</i>
284	<i>Propuestas Estratégicas e Institucionales</i>
285	<i>El Imperativo de la Gobernanza Humana</i>
286	La Revolución en los Asuntos Militares (RAM) y la Disrupción Digital
286	<i>La Interdependencia Compleja y la Erosión del Enclave Territorial</i>
287	<i>Las Operaciones Multi-Dominio (MDO)</i>
287	<i>Análisis Multidimensional de las Tecnologías en el Teatro Operativo Futuro</i>

288	<i>Inteligencia Artificial y la Algoritmización del Mando y Control</i>
288	<i>Sistemas Autónomos Letales (LAWS) y la Guerra de Enjambres</i>
289	<i>El Ciberespacio y el Espectro Electromagnético como Vectores Dominantes</i>
290	<i>La Guerra Cognitiva y de la Información: El Cerebro Humano como Escenario Operativo</i>
291	<i>Logística Avanzada, Sostenibilidad y la Resiliencia Industrial en el Frente del Futuro</i>
291	<i>Implicancias Éticas, Jurídicas y Geopolíticas de la Digitalización Militar</i>
292	<i>El Derecho Internacional Humanitario frente a la Autonomía Militar</i>
292	<i>La Asimetría Norte-Sur y la Brecha Tecnológica Regional</i>
293	Conclusión
293	Referencias

297 **CAPÍTULO UNDÉCIMO. PERÚ, CENTRO DE ALTOS ESTUDIOS NACIONALES DE PERÚ (CAEN). DE LO FÍSICO A LO COGNITIVO: NUEVAS TECNOLOGÍAS Y LA REDEFINICIÓN DEL CAMPO DE OPERACIONES**

Juan Fernando Ormachea Montes

298	Introducción
299	Evolución del campo de operaciones: De lo físico al multidominio y cognitivo
299	<i>La transformación de los tradicionales principios de la guerra:</i>
301	<i>La virtualización de las fases iniciales del combate: drones, ataques remotos y nuevas formas de contacto operacional</i>
302	Tecnologías emergentes y su impacto en el campo de operaciones
303	<i>Inteligencia Artificial (IA): Decisiones inmediatas y la guerra algorítmica</i>
305	<i>El Ciberespacio: el nuevo dominio invisible del conflicto</i>
306	<i>Sistemas no tripulados y enjambres: La redefinición de la masa y el riesgo</i>
307	Big Data y analítica avanzada: la supremacía de la información
308	Tecnologías espaciales: la dependencia estratégica del dominio orbital
310	<i>La expansión de los dominios operacionales y la centralidad de los sistemas C4ISR</i>
313	De la guerra física a la guerra cognitiva: La transformación del concepto de operaciones
315	Implicancias para la seguridad y defensa nacional

316 Conclusões y reflexiones

318 Referências

319 CAPÍTULO DUODÉCIMO. PORTUGAL. INSTITUTO DA DEFESA NACIONAL (IDN). TECNOLOGIA, DOCTRINA E ENSINO MILITAR PROFISSIONAL NO CAMPO DE BATALHA TRANSPARENTE. TECNOLOGIA NO CAMPO DE BATALHA MODERNO, ADAPTAÇÃO DOCTRINÁRIA E ENSINO, FORMAÇÃO E TREINO MILITARES

Luís Fernando Machado Barroso

Pedro Nuno Antunes Ferreira

320 Introdução

323 O campo de batalha transparente: visibilidade, letalidade e compressão temporal

325 Tecnologia e doutrina: entre aceleração, adaptação e transformação

327 Adaptações doutrinárias: reformular a guerra de manobra

329 Adaptações operacionais: comando, logística, guerra eletrônica e sustentação

332 Adaptações culturais e estruturais: da eficiência burocrática à aprendizagem adaptativa

333 O ensino, a formação e o treino militares como motor da adaptação

336 Implicações curriculares para educação, formação e treino de oficiais

338 Das funções de combate à transformação institucional

341 Proposta integrada de adaptação

342 Riscos de adaptação incompleta e critérios de implementação

344 A formação do oficial no centro da transformação

346 Um modelo pedagógico para a adaptação contínua

348 Conclusão

349 Bibliografia

351 CAPÍTULO DECIMOTERCERO. URUGUAY. CENTRO DE ALTOS ESTUDIOS NACIONALES (CALEN). LA INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS EN LOS ESCENARIOS DE OPERACIONES FUTURAS, IMPLICANCIAS DESDE LA PERSPECTIVA DEL COLEGIO DE DEFENSA DEL URUGUAY -CALEN

Alfonso Fojo

352	Introducción
354	Abordaje metodológico
355	Limitaciones al Estudio
355	<i>Para la redacción del trabajo se situó en trabajo en el nivel Político Estratégico:</i>
356	Marco teórico y conceptual
356	<i>Marco teórico</i>
357	<i>Marco conceptual</i>
359	<i>Materiales avanzados y manufactura encontrándose en ellos</i>
359	<i>Inteligencia artificial, computación y comunicaciones</i>
360	<i>Energía y medio ambiente</i>
360	<i>Tecnologías cuánticas</i>
360	<i>Biotecnología y vacunas</i>
361	<i>Sensores, navegación y temporización</i>
361	<i>Defensa, espacio, robótica y transporte</i>
361	Entorno Estratégico Global
364	Características de la República Oriental del Uruguay (ROU)
366	Análisis y discusión sobre el impacto de las EDT en los entornos operativos
366	<i>Inteligencia Artificial y aprendizaje automático</i>
367	<i>Sistemas autónomos y robóticos</i>
368	Computación cuántica y ciberdefensa
368	<i>Redes de nueva generación (5G/6G), IoT militar y computación de borde</i>
369	<i>Armas hipersónicas, energía dirigida y dominio espacial</i>
369	<i>Dominio cognitivo e informacional</i>
370	<i>Impactos transversales en los entornos operativos</i>
371	Escenarios prospectivos de operaciones futuras
374	Síntesis de los escenarios
374	Síntesis del impacto asociados a entornos operativos futuros
375	Conclusiones
377	Recomendaciones
380	Bibliografía



PRÓLOGO

Miguel Ballenilla y García de Gamarra

La historia de los conflictos demuestra que la tecnología ha acompañado de forma permanente la evolución de la guerra. Desde los primeros instrumentos concebidos para ampliar la capacidad del combatiente hasta los actuales sistemas autónomos, las redes digitales y las aplicaciones militares de la inteligencia artificial, cada avance científico y tecnológico ha contribuido a modificar los medios, los procedimientos y los escenarios en los que los Estados y otros actores confrontan sus intereses y voluntades.

Sin embargo, pocas etapas de la historia reciente han conocido una aceleración tecnológica comparable a la actual. La convergencia de la inteligencia artificial, los sistemas autónomos y no tripulados, la robótica, las tecnologías espaciales, la computación avanzada, la biotecnología, la analítica masiva de datos y las nuevas capacidades de actuación en el ciberespacio están transformando profundamente el entorno estratégico. Tecnologías que hace apenas unos años pertenecían al ámbito de la prospectiva, hoy forman parte de operaciones reales, mientras otras evolucionan a una velocidad que desafía los tradicionales ciclos de planeamiento, adquisición de sistemas, desarrollo doctrinal y formación.

En este contexto se enmarca el presente Tomo XV de la Asociación de Colegios de Defensa Iberoamericanos, dedicado a **«La influencia de las nuevas tecnologías en los escenarios de operaciones futuros»** y presentado con ocasión de la XXVII Conferencia de Directores de Colegios de Defensa Iberoamericanos en el Centro Superior de Estudios de la Defensa Nacional de España.

La elección del tema difícilmente podría ser más oportuna. Los conflictos contemporáneos ponen de manifiesto que la tecnología ha dejado de constituir únicamente un elemento de apoyo o un multiplicador de capacidades. En numerosos ámbitos se ha convertido en un factor determinante para alcanzar la

superioridad operacional, reducir los tiempos para la toma de decisiones y producir efectos simultáneos en los dominios físicos y en los no físicos.

El campo de operaciones se extiende hoy desde los dominios terrestre, marítimo y aéreo hasta el espacial y el ciberespacio, incorporando además el espectro electromagnético, el entorno de la información y la dimensión cognitiva como ámbitos de creciente competición. En este entorno emerge con especial fuerza la inteligencia artificial. Su incorporación a los procesos de inteligencia, vigilancia y reconocimiento, al mando y control, a la logística, al análisis predictivo y a los sistemas de armas abre posibilidades hasta hace poco difícilmente imaginables. La capacidad para procesar grandes volúmenes de datos y transformarlos en información útil puede acelerar el ciclo de decisión y conectar sensores, toma de decisiones y sistemas productores de efectos con una eficacia sin precedentes.

Pero la inteligencia artificial plantea igualmente profundos interrogantes. La automatización de determinadas funciones militares y la progresiva autonomía de los sistemas exigen una reflexión rigurosa sobre sus límites. La fiabilidad de los datos, los sesgos de los modelos, la vulnerabilidad frente al engaño, la trazabilidad de las decisiones y la responsabilidad derivada de su empleo adquieren una relevancia extraordinaria cuando las consecuencias pueden afectar directamente a la vida humana y a la aplicación de los principios jurídicos y éticos que rigen los conflictos armados.

Sin embargo, la superioridad técnica, por sí sola, no garantiza el éxito estratégico. Disponer de sistemas más avanzados no sustituye al pensamiento crítico, al liderazgo, al conocimiento del adversario ni a la capacidad de comprender la naturaleza política del conflicto. La guerra continúa siendo una confrontación entre voluntades y las decisiones humanas permanecen en el centro de la estrategia.

De ahí que uno de los principales valores de esta obra sea la atención concedida al factor humano. La velocidad de evolución de la tecnología convierte la formación en una auténtica capacidad estratégica. Ya no resulta suficiente preparar a los profesionales de la defensa para operar sistemas concretos; es necesario desarrollar organizaciones capaces de aprender, cuestionar sus procedimientos y adaptarse permanentemente.

En este sentido, la aparición de la inteligencia artificial generativa introduce también nuevas cuestiones en el ámbito de la enseñanza y de la producción del conocimiento en defensa. Estas herramientas pueden ampliar las posibilidades de investigación y apoyar los procesos educativos. Al mismo tiempo, obligan a reforzar la alfabetización tecnológica, la capacidad de evaluación crítica y la autonomía intelectual.

Esta reflexión guarda una relación directa con otro de los grandes desafíos presentes en la obra: la soberanía tecnológica. El desarrollo desigual de las tecnologías disruptivas puede ampliar las diferencias de capacidad entre Estados y generar nuevas formas de dependencia. Las infraestructuras digitales, los semiconductores, los sistemas espaciales, las plataformas de inteligencia artificial, las comunicaciones avanzadas y las cadenas de suministro de componentes críticos son cada vez más elementos vinculados a la autonomía estratégica y a la resiliencia nacional.

Para Iberoamérica, esta realidad presenta riesgos evidentes, pero también oportunidades. La región no puede contemplar la transformación tecnológica exclusivamente desde la posición de consumidora de soluciones desarrolladas por terceros. Reducir las brechas existentes requiere políticas sostenidas de educación, investigación e innovación; una mejor conexión entre las Fuerzas Armadas, las universidades, los centros de pensamiento y el tejido industrial; y una visión estratégica capaz de identificar aquellos ámbitos en los que resulte posible desarrollar capacidades propias o compartidas.

La cooperación constituye, por ello, un elemento esencial. Ningún país puede afrontar aisladamente la totalidad de los desafíos derivados de la actual transformación tecnológica. La interoperabilidad, el intercambio de conocimiento, la formación conjunta y la construcción de marcos de confianza adquieren una importancia creciente ante amenazas que ignoran fronteras y explotan la conectividad global.

Una de las riquezas del presente volumen reside precisamente en la pluralidad de las perspectivas que reúne. Las aportaciones procedentes de Brasil, Ecuador, El Salvador, España, Honduras, México, Paraguay, Perú, Portugal y Uruguay reflejan experiencias, necesidades y aproximaciones diferentes, pero permiten reconocer importantes preocupaciones comunes. La inteligencia artificial, las operaciones multidominio, los sistemas autónomos, la ciberdefensa, la pro-

tección de las infraestructuras críticas, la guerra cognitiva, la interoperabilidad, el desarrollo doctrinal y la formación aparecen de manera recurrente a lo largo de la obra.

Las investigaciones reunidas en este volumen comparten asimismo una clara dimensión prospectiva. Pensar sobre los escenarios de operaciones futuros no significa pretender predecir el porvenir con exactitud. Significa identificar tendencias, incertidumbres y posibles discontinuidades para mejorar las decisiones del presente.

El debate que plantea esta obra no es, por tanto, únicamente tecnológico. Es un debate estratégico. Nos obliga a preguntarnos qué capacidades necesitan nuestros Estados, qué dependencias estamos dispuestos a asumir, cómo debemos preparar a nuestros profesionales y qué principios deben orientar el empleo de las nuevas tecnologías. Nos invita igualmente a analizar el papel de las instituciones de enseñanza superior de la defensa en un momento en el que el conocimiento se convierte, más que nunca, en un componente esencial del poder nacional.

La Asociación de Colegios de Defensa Iberoamericanos constituye un foro privilegiado para desarrollar esta reflexión. Su capacidad para reunir diferentes tradiciones, experiencias y perspectivas permite abordar los grandes retos de la seguridad y la defensa desde una mirada compartida. En un tiempo de fragmentación y competición creciente, mantener estos espacios de diálogo académico y estratégico resulta necesario.

El presente Tomo XV es una expresión de ese compromiso. Sus autores no ofrecen respuestas únicas ni soluciones definitivas a un fenómeno que continúa evolucionando mientras es estudiado. Ofrecen análisis, preguntas y perspectivas que permiten comprender mejor la magnitud de la transformación en curso y contribuyen a preparar a nuestras instituciones para escenarios todavía inciertos.

Porque, en último término, la tecnología proporciona capacidades; es el ser humano quien les otorga propósito. Y serán el conocimiento, el liderazgo, la ética y la visión estratégica los que determinen cómo afrontar la extraordinaria transformación tecnológica que hoy presenciamos.

Con esta reflexión se invita al lector a adentrarse en las páginas de la presente obra.



Madrid 8 julio 2026



CAPÍTULO PRIMERO

BRASIL, ESCOLA SUPERIOR DE GUERRA (ESG)

Las nuevas tecnologías y el futuro de la guerra

Ricardo Rodrigues Freire

Resumen: Ante los constantes avances tecnológicos en la actualidad y su creciente influencia sobre la guerra, este texto analiza la presencia de tecnologías disruptivas en el ámbito militar e intenta inferir sus impactos en los conflictos bélicos actuales y futuros. La investigación se desarrolla siguiendo una metodología analítico-deductiva, con un recorte espacial amplio y un enfoque cronológico en el siglo XXI, con mirada en los escenarios futuros, pese a su ambigüedad. La investigación se sustenta en la bibliografía tradicional de los Estudios Estratégicos, en la información contenida en fuentes oficiales abiertas, así como en los datos recopilados en revistas especializadas de la industria de Defensa. Para alcanzar los objetivos propuestos, el trabajo se centró en la definición del concepto “guerra”, optando por la visión “clausewitziana” y la fidelidad a la Polemología. Asimismo, analizó las implicaciones de las tecnologías emergentes en los conflictos (actuales y futuros), con énfasis en la capacidad estatal de crear y aplicar estas innovaciones en los campos de batalla. Además, presenta conclusiones sobre la evolución del *modus operandi* del combate, frente a los cambios tecnológicos, subrayando que la naturaleza política y estratégica de la guerra permanece inalterada y sumamente dependiente del factor recursos humanos, civiles y militares – “la piedra angular” desde la concepción de una nueva arma hasta su empleo efectivo.

Palabras clave: Guerra, Futuro (de las guerras), Tecnologías, Disrupción, Defensa.

Acerca del autor: Ricardo Rodrigues Freire. Doctor en Ciencia Política por el Instituto de Estudios Sociales y Políticos de la Universidad del Estado de Río de Janeiro; Magíster en Estudios Estratégicos de la Defensa y de la Seguridad por el Instituto de Estudios Estratégicos de la Universidade Federal Fluminense. Coronel retirado del Ejército Brasileño, miembro del Cuerpo Permanente de la Escola Superior de Guerra (ESG), donde se desempeña como Analista del Centro de Estudios Estratégicos Mariscal Cordeiro de Farias y como Coordinador Académico de la ESG ante la Asociación de Colegios de Defensa Iberoamericanos

Aspectos introductorios

La guerra es un fenómeno central en la historia de la humanidad. Keegan (2006), al escribir *“Uma história da Guerra”*, afirma que los períodos de paz constituyen excepciones en la trayectoria humana. Tipifica la guerra como un fenómeno social responsable de moldear instituciones y valores a lo largo del tiempo, y también de impulsar una continua evolución tecnológica.

Actualmente, el mundo ha comenzado a experimentar una nueva era de desarrollo, con características esencialmente tecnológicas. En términos meramente didácticos, la presente “ola” fue clasificada por Kon (2020) como “la cuarta ola”, posterior a las tres anteriores: la agraria, la industrial mercantilista y la del conocimiento, tal como fueron definidas por Toffler (1981).

Se observa, pues, en el tiempo presente, una significativa dinámica de avances tecnológicos, enmarcando un fenómeno que ha afectado sobremanera a la humanidad, inclusive en la forma de conducir la guerra, puesto que, conforme afirma Kon (2020, p. 188), “todo se ha vuelto 4.0”. Y, no está de más añadir, ya se avanza hacia un nuevo mundo “5.0”.

En este diapasón, el presente texto se propone analizar la presencia de nuevas tecnologías en el ámbito de los instrumentos de la Defensa Nacional y busca inferir cómo tales innovaciones influyen, e influirán, en los conflictos bélicos actuales y futuros.

Para ello, el contenido aquí presentado es fruto de una investigación desarrollada según una metodología analítico-deductiva, con un amplio recorte espacial y enfoque temporal en el presente siglo, sin desatender la visualización de escenarios futuros, pese a las incertidumbres actualmente existentes. Se con-

sidera que no resulta exagerado enfatizar que el mundo es cada día más incierto, además de volátil, complejo y ambiguo, tal como Whiteman (1998) describió los campos de batalla a finales del siglo pasado.

Para alcanzar el objetivo propuesto, el contenido textual fue dividido, además de estos aspectos introductorios, en otras cuatro secciones. La primera de ellas se propone decodificar la guerra y esclarecer sobre qué fenómeno se están explorando los efectos de las nuevas tecnologías. A continuación, se abordan algunas de las nuevas tecnologías que vienen impactando y que, posiblemente, impactarán las contiendas futuras. Posteriormente, se aborda la repercusión de estas nuevas tecnologías en el desarrollo de las guerras del porvenir, con la mirada puesta en la capacidad del poder estatal para desarrollar, producir y emplear tales innovaciones en el campo de batalla.

En conclusión, el texto, de manera deductiva, se posiciona respecto al mantenimiento de las características político-estratégicas de las guerras, pese a las significativas transformaciones en la forma de combatir, debido a las innovaciones tecnológicas, destacando la relevancia del factor humano en todas las etapas que circundan las disrupciones tecnológicas, desde su génesis hasta su empleo.

Decodificación de la guerra

Antes de abordar las nuevas tecnologías y el futuro de las guerras, resulta prudente esclarecer el tipo de fenómeno que se pretende considerar. La principal razón de esta cautela es la frecuente distorsión del concepto de “guerra” y las implicaciones de dicha práctica.

Se observa que, en la actualidad, ha sido común la difusión de expresiones como “guerra contra las drogas”, “guerra contra el crimen organizado”, entre otras. No obstante, no es posible olvidar que la guerra es tan antigua como la humanidad, antecediendo al Estado, a la diplomacia y a la estrategia, como sostiene Keegan (2006). Por lo tanto, antes de intentar calificar el fenómeno de la guerra, es necesario comprender su verdadero significado, es decir, descifrar un concepto ya consagrado a lo largo del tiempo, sin correr el riesgo de corromperlo.

Según la perspectiva “clauswitziana”, la guerra constituye un fenómeno esencialmente político, que continúa la actividad política por otros medios (Clausewitz, 1984). Pese a la existencia de visiones divergentes de la de Clausewitz, como la de Foucault (2012), por ejemplo, quien entiende la política como una visión continuada de la guerra constante que impregna la convivencia social, el presente texto se fundamenta en el primer postulado.

Así pues, por tratarse de un fenómeno político, la guerra es impulsada por entes políticos que cuentan con medios coercitivos y con la legitimidad para utilizarlos: en teoría, los Estados. Sin embargo, otros actores no estatales, motivados por objetivos políticos, también pueden recurrir al uso de la fuerza para alcanzar sus propósitos.

En este diapasón, la complejidad del fenómeno bélico dio origen a una rama de la ciencia dedicada exclusivamente al estudio de la guerra: la Polemología. En este campo epistemológico, se diagnosticaron primordialmente dos tipos de guerra: la regular (o convencional) y la irregular (no convencional).

La primera se caracteriza por el enfrentamiento entre Estados nacionales, debidamente “regidos” por las normas del Derecho Internacional. La otra, por su parte, es propia del enfrentamiento entre Estados y grupos “subestatales”, con una nítida discrepancia de capacidades entre los contendientes, hecho que motiva el empleo, por parte del actor menos favorecido, de técnicas propias de la guerrilla, el sabotaje y el terrorismo (Fayal y Freire, 2024, p. 41-43). Aun así, es importante subrayar que los citados autores destacan la motivación política como rasgo significativo y punto en común de los dos modelos aquí tipificados.

Sin embargo, como los conflictos armados son fruto de “fuerzas vivas” (Clausewitz, 1984, p. 78), es legítimo que la Polemología evolucione y considere otras ramificaciones de la guerra. Así, más recientemente, se han admitido algunas derivaciones del concepto básico. Entre ellas, la “guerra proxy” o “guerra por delegación”, definida por Freire y Fayal (2024, p. 49, traducción propia) como “conflictos en los cuales una potencia (o grupo de potencias) no se involucra directamente en los combates, sino que apoya a otras fuerzas — Estados, grupos rebeldes u organizaciones — que luchan conforme a objetivos trazados por la potencia (o coalición)”.

Asimismo, se observa la idea de “guerra asimétrica” para encuadrar, en el contexto de las guerras convencionales, los conflictos entre Estados con capacidades excesivamente dispares, tal como lo describe Paul (1994, p. 20). En tal contexto, debido a la carencia de medios, la forma de combatir del actor más débil se asemeja a aquellas propias de las guerras irregulares, pese al sesgo convencional del fenómeno.

Además, con el advenimiento del uso cada vez más intenso del espacio cibernético, o ciberespacio, la Polemología pasa a considerar el concepto de “guerra cibernética”. Esta nueva versión fue definida por Arquilla y Ronfeldt (1993, p. 30, traducción propia) como “ciberguerra”, en los siguientes términos:

“[...] Se refiere a conducir, y prepararse para conducir, operaciones militares de acuerdo con principios relacionados con la información. Significa perturbar, cuando no destruir, los sistemas de información y comunicación, definidos ampliamente hasta el punto de incluir la cultura militar, de los cuales un adversario depende para “conocerse” a sí mismo [...] intentar saberlo todo sobre un adversario mientras este no sabe nada sobre nosotros [...] inclinar el “equilibrio de información y conocimiento” a nuestro favor, sobre todo cuando el equilibrio de fuerzas no lo es [...] utilizar el conocimiento para que se empleen menos capital y mano de obra. Esta forma de guerra puede involucrar diversas tecnologías — notablemente para C3I¹; para recopilar, procesar y distribuir inteligencia; para comunicaciones tácticas, posicionamiento e identificación de amigos y enemigos (IFF)²; y para sistemas de armas “inteligentes” [...] el *blinding* [cegamiento], el *jamming* [bloqueo], el engaño, la sobrecarga y la intrusión electrónicas de los circuitos de información y comunicación del adversario”.

Asimismo, se incorporó el concepto de “guerra híbrida” al conjunto de los estudios polemológicos. Según Freire y Fayal (2024, p. 58), se trata de “una evolución de las estrategias de conflicto que combinan métodos convencionales y no convencionales, mezclando operaciones militares regulares e irregulares”,

¹ Comando, control, comunicación e inteligencia (nota del autor).

² Abreviatura de la expresión inglesa: Identification Friend or Foe (nota del autor).

considerando, por ejemplo, el empleo masivo de “ciberataques y campañas de desinformación”. Los citados autores enfatizan que la “guerra híbrida” condensa todos los conceptos de guerra estudiados por la Polemología.

Sin embargo, debe considerarse la existencia de rasgos histórico-culturales que influyen en la decodificación de la guerra. Nótese que, conforme se lee en Saint-Pierre (2013, p. 32), en la Antigua Grecia, la guerra, o *pólemos*, era descodificada como el conflicto armado externo con pueblos “no griegos”. Internamente, las “discordias, subversiones o revueltas” eran denominadas *metábole* o *stasis*. Y, para cada tipo de contienda, los medios empleados eran distintos. Resulta lícito, por lo tanto, inferir que la génesis de las fuerzas armadas y de las fuerzas policiales proviene de esa tradición.

De este legado griego surge la importante idea desarrollada por Carl Schmitt (1888-1985), quien considera al oponente en la guerra como un “enemigo” y, por consiguiente, en la búsqueda de la victoria, los adversarios pueden ser sumariamente eliminados. Además, en las relaciones con el enemigo, se consideran las hipótesis de rendición y de celebración de tratados de paz (Schmitt, 2008).

Ante tales argumentos, surgen las siguientes dudas:

¿Es procedente aplicar el constructo de Schmitt (2008) a los transgresores de las normas legales?

- ¿Existe razonabilidad en las acciones de eliminación sumaria, rendirse o promover armisticios con actores movidos por intereses distintos, principalmente económicos, desprovistos de motivación política orientada a la conquista del poder y al dominio del Estado?

Se considera que no. Se entiende, por lo tanto, que la represión de los actos criminales cometidos por delincuentes, tales como los traficantes de drogas ilícitas, por ejemplo, es de competencia estricta de las autoridades policiales.

Por supuesto, como fruto de la realidad contemporánea, no se descarta la posibilidad de que las fuerzas armadas actúen en apoyo de los instrumentos policiales en la represión de las ilicitudes, pero ello no implica calificar la acción emprendida como “guerra”. Se sostiene la visión de que la distorsión del vocablo “guerra”, fruto de modismos e intereses ocultos, puede tener efectos dele-

téoros sobre el orden interno de los Estados y sobre el sistema internacional en su conjunto.

Así pues, para el análisis de las nuevas tecnologías que influirán en las peleas del futuro, es necesario dejar explícito que las “guerras” aquí analizadas serán aquellas derivadas de la extensión de la acción política por medios coercitivos, excluyéndose, por lo tanto, los fenómenos resultantes de distorsiones consideradas inadecuadas a los presupuestos teóricos esbozados en este trabajo.

Las principales tecnologías que despuntan en el escenario de las guerras

Desde la Antigüedad, la ciencia y la tecnología moldean el material bélico y la capacidad de imposición de la voluntad militar. Asimismo, las evoluciones en el campo de la ciencia, la tecnología y la innovación constituyen aspectos determinantes en las guerras, pues, como afirma Crevelde (2016, traducción propia), “la guerra es una actividad libre y creativa, basada en fundamentos científicos”.

Recientemente, los avances tecnológicos más significativos experimentados por la humanidad han sido denominados “disruptivos”. Este término tiene su origen en las ciencias económicas y de gestión, y es definido por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) como una innovación que impacta los mercados y las actividades económicas, desplazando paradigmas anteriores (OCDE, 2005).

Dichos avances tecnológicos disruptivos desencadenan verdaderas revoluciones en la industria. La conocida Cuarta Revolución Industrial, conforme a la definición propuesta por Schwab (2016), se fundamenta en: inteligencia artificial (IA), robótica, nanotecnología, sistemas autónomos, biotecnología y guerra cibernética.

Para contextualizar, cabe destacar que esta Cuarta Revolución fue precedida por aquellas sostenidas por la mecanización impulsada por el vapor, en la producción en serie de las líneas de montaje y en la informatización. Asimismo,

dado que la guerra se encuentra cada vez más respaldada por la industria³, el dominio de estas tecnologías, a lo largo de la historia, ha propiciado —y continúa propiciando— ventajas militares decisivas, rediseñando el arte de la guerra.

Desde la perspectiva de Gavião y Kostin (2024, p. 114), en el contexto militar, las tecnologías disruptivas son aquellas que generan nuevas características para el combate, en particular mediante la explotación de herramientas avanzadas de la era digital y otorgando superioridad a los actores que las dominan.

Así, esta sección abordará las tecnologías disruptivas que han venido adquiriendo protagonismo en los conflictos bélicos recientes, así como los principales actores involucrados en la investigación y el desarrollo de tales innovaciones. También, examinará la aplicación concreta de dichas innovaciones en los campos de batalla contemporáneos y, por inferencia, en los futuros.

En esta línea, surge la siguiente cuestión:

- ¿Cuáles son las principales tecnologías disruptivas que impactan las guerras en la actualidad?

Gavião y Kostin (2024), en un análisis minucioso, enumeran las siguientes: la IA, los *drones* y los vehículos no tripulados⁴ la robótica; la cibernética; los sistemas autónomos y las armas autónomas letales (LAWS); los satélites y los medios de empleo en el espacio; la nanotecnología; y la biotecnología.

Según la descripción de los citados autores (Gavião y Kostin, 2024, pp. 115-117), sobre cada una de las tecnologías enumeradas, la IA ha sido ampliamente empleada en sistemas de vigilancia, reconocimiento, mando y control, logística,

³ Cabe señalar que Francia, por ejemplo, posee en su estructura organizacional de Defensa una Dirección General de Armamento (DGA) “agencia gubernamental de tecnología y adquisiciones de defensa, responsable del desarrollo y la gestión de proyectos, así como de la adquisición de sistemas de defensa para las Fuerzas Armadas de Francia” (FIERGS, 2020, traducción propia). Asimismo, aquí en Brasil, el Ministerio de Defensa de Brasil ha venido realizando esfuerzos para estructurar y desarrollar la denominada Base Industrial de Defensa (Brasil, 2025).

⁴ Se observa aquí, por parte de los autores, la adhesión al estándar estadounidense de clasificar como dron únicamente los vectores aéreos, reservando para los terrestres y acuáticos la denominación de vehículos no tripulados. Tal perspectiva no constituye un consenso global (nota del autor).

operaciones cibernéticas y vehículos no tripulados (incluidos los *drones*). Sus aplicaciones permiten el procesamiento de un volumen significativo de datos, facilitando la toma de decisiones humanas y autónomas en situaciones de combate.

Los sistemas de IA, principalmente debido a los avances experimentados en la computación cuántica, han evolucionado con extrema rapidez, y su aprovechamiento en los sistemas militares se vuelve cada vez más frecuente, ya sea en la robótica, en las armas autónomas, en la configuración de redes neuronales, en el uso de lógica difusa, entre otras posibilidades.

Por su parte, los *drones* y demás vehículos no tripulados —que, en términos prácticos, comprenden vectores aéreos, terrestres, acuáticos y subacuáticos— han revolucionado el campo de batalla, permitiendo la ejecución de misiones de reconocimiento y ataques de precisión, muchas veces mediante operaciones tipo “enjambre”. Se destacan por su capacidad de operación autónoma en distintos dominios, orientados por IA y con el empleo de diversos armamentos.

Estos equipos posibilitan la conducción de operaciones militares que provocan importantes bajas a la fuerza oponente, prácticamente sin riesgos para el plantel del atacante. Además, constituyen vectores capaces de causar pérdidas y daños a los medios enemigos de considerable costo de producción e importancia estratégica, mediante artefactos de valor relativamente bajo.

En lo que respecta a la robótica militar, los *robots* han sido empleados en tareas de desminado, reconocimiento, combate y apoyo logístico. Su integración con herramientas de IA mejora la autonomía y la eficacia de estos equipos. Particularmente, en las operaciones de desminado, en las cuales los riesgos de bajas son elevados —lo que hace que el trabajo sea extremadamente lento—, la robótica demuestra ventajas significativas.

En lo que concierne al dominio del ciberespacio, mediante la cibernética (también con el auxilio de la IA), se vislumbran avances en una dinámica frenética. Los ataques cibernéticos, o ciberataques, deterioran sistemas de inteligencia y provocan colapsos en infraestructuras críticas y en los sistemas de comunicaciones del adversario. La guerra cibernética se caracteriza, en muchas ocasiones, por la dificultad de identificar el origen de la acción adversa, lo que exige

el desarrollo de nuevas capacidades de defensa y también de reacción inmediata frente a las acciones hostiles provenientes del entorno digital.

Las plataformas dotadas de autonomía y las denominadas armas autónomas letales (LAWS), por su parte, son sistemas sofisticados capaces de identificar, seleccionar y atacar objetivos sin intervención humana directa. Esta constituye un área sensible de la Polemología, objeto de amplios debates multidisciplinarios, ya que suscita cuestiones éticas y jurídicas relativas a la responsabilidad por las acciones emprendidas. Las facultades autonómicas de las LAWS que involucran la eliminación de la vida humana constituyen un tema sumamente controvertido en la actualidad.

Pasando al dominio espacial, los modernos satélites equipados con IA y dotados de brazos robóticos – obsérvese aquí la integración de la IA, la robótica y otras tecnologías – son utilizados para vigilancia, comunicación, navegación e incluso para la remoción de desechos espaciales. Además, su empleo como armas “anti satélite” resulta plausible y constituye un interés inminente para las potencias que actúan en esta dimensión.

Por último, la nanotecnología y la biotecnología poseen aplicaciones emergentes y se integran con las demás tecnologías disruptivas. Estas incluyen el desarrollo de materiales avanzados para la confección de uniformes, el blindaje de los medios y la fabricación de sensores miniaturizados, así como el empleo de agentes biológicos en las operaciones militares, ya sea para la protección del personal –en la medicina militar, por ejemplo– o para provocar limitaciones o bajas en el oponente.

Todo lo expuesto hasta aquí permite, siguiendo la línea de razonamiento propuesta en este trabajo, enumerar los países que se destacan en la innovación tecnológica disruptiva en el ámbito militar. No obstante, antes de mencionarlos, cabe señalar que el dominio de las innovaciones tecnológicas disruptivas es consecuencia de una opción político-estratégica. Se hace necesario invertir en la capacitación de recursos humanos y en la realización de investigaciones para alcanzar resultados. Y ello no ocurre a corto plazo. Se trata de proyectos que se extienden durante décadas, susceptibles al fracaso y que, por esa razón, normalmente demandan apoyo estatal.

Al nombrar a los protagonistas de la disrupción en el contexto castrense, Gavão y Kostin (2024, p. 117-131) señalan el protagonismo de los Estados Unidos (EE.UU.), de la República Popular China (RPC), de Rusia, de Israel, de Turquía y de Irán. Basados en fuentes especializadas⁵, los citados autores señalan que Estados Unidos es líder en investigación, desarrollo y aplicación de IA, *drones*, robótica y guerra cibernética.

Se destacan algunos proyectos, como el *Sea Hunter* (navío autónomo), el *Rip-saw M5* (vehículo terrestre no tripulado), el F-35 Lightning II (caza con IA integrada) y las constelaciones de satélites inteligentes. El Departamento de Defensa de los Estados Unidos ha invertido anualmente miles de millones de dólares en investigaciones relacionadas con la IA y, para ello, mantiene una estructura estatal dedicada al tema: el *Chief Digital and Artificial Intelligence Officer* (CDAO). El CDAO tiene como atribución principal acelerar la adopción de tecnologías disruptivas en favor de la Seguridad Nacional.

Pasando a la República Popular China, el país también desarrolla proyectos fundamentados en IA y ha avanzado en la producción de *drones* armados, sistemas robóticos y satélites autónomos. Es el mayor exportador mundial de *drones* armados y líder en patentes de IA. Empresas como *Huawei*, *Alibaba* y *Tencent* invierten fuertemente en investigación y desarrollo de tecnologías orientadas al empleo militar. Sistemas como el *Blowfish A2* (*drone* helicóptero), el *Sharp Claw I* (*dron* terrestre) y el *Marine Lizard* (vehículo anfibio autónomo) constituyen ejemplos de innovación china en este sector.

Por su parte, Rusia, principalmente en razón del conflicto con Ucrania, invierte en proyectos que se valen de la IA para la operación de sistemas de defensa antiaérea (*Pantsir-SM*), la producción de *drones* pesados (*Sukhoi S-70 Okhot-nik*), de torpedos nucleares autónomos (*Poseidon*) y de equipos orientados a la

⁵ Cabe destacar aquí que la información presentada ha sido obtenida de fuentes abiertas y, en muchos casos, basada en informaciones oficiales y/o proporcionadas a publicaciones especializadas por los fabricantes de los equipos. Se considera la posibilidad de omisión de datos, en virtud del sigilo que, en general, los Estados otorgan al tema. Además, resulta plausible la práctica de sobrevalorar algunos de los productos presentados, debido a intereses comerciales de los fabricantes y a objetivos disuasorios por parte de los Estados. Asimismo, debe considerarse que algunos productos aún pueden encontrarse en fase de proyecto y/o prototipo, con resultados prácticos no (o no debidamente) mensurados y, por lo tanto, con eficacias cuestionables (nota del autor).

guerra electrónica (*RB-109A Bylina*). Asimismo, se subraya el uso de IA en la guerra cibernética y electrónica, además del amplio empleo de vehículos autónomos, los cuales constituyen rasgos distintivos de la actuación de las fuerzas armadas rusas en el conflicto con los ucranianos.

Israel, otro Estado también involucrado en conflictos armados recientes, es reconocido desde hace mucho tiempo por su capacidad de investigación y aplicación intensiva de IA en *drones* militares, especialmente en el contencioso de la Franja de Gaza y sus desdoblamientos. Los israelíes desarrollaron sofisticados sistemas de selección de objetivos basados en IA, como el *Lavender*, y emplean *drones* armados y sistemas de defensa antimisiles dotados de un elevado grado de avance tecnológico.

Por último, cabe comentar sobre Irán, Turquía e India, países con capacidades emergentes para el desarrollo de tecnologías avanzadas en la producción y exportación de *drones* armados y sistemas autónomos, muchos de ellos a costos relativamente bajos. Tal hecho resulta relevante, puesto que ha ampliado el acceso a tecnologías disruptivas por parte de actores regionales y no estatales, dando lugar a la conocida “asimetría inversa”⁶.

En lo que respecta a India, merece subrayo su notorio protagonismo en el dominio espacial, alcanzando niveles de desarrollo bastante próximos a los de reconocidas potencias del sector, como Estados Unidos, la República Popular China y Rusia (Rajagopalan; Stroikos, 2024).

Dicho esto, al analizar los conflictos bélicos más recientes, se observa que, ya a principios de este siglo, la Guerra de Afganistán (2001-2021) constituyó un escenario emblemático para el empleo de herramientas de IA destinadas a la predicción de ataques insurgentes, conforme señala Spahr (2024).

Si se analiza el segundo enfrentamiento Armenio-Azeri (2020), se observa que el uso de *drones* conjugados con herramientas de IA fue decisivo para el éxito

⁶ Según consta en Friede (2010, pp. 158-159, traducción propia), “la noción central de ‘Guerra Asimétrica Inversa’ podría traducirse como todo y cualquier tipo de conflicto bélico en el que, al menos en algún momento, exista una efectiva limitación (o, en términos más precisos, ‘autolimitación’) del empleo de la evidente superioridad militar (y, particularmente, tecnológica) en el campo de batalla”.

azerí en la región del Cáucaso, como afirman Gavião y Kostin (2024, pp. 132-133).

Pasando a los conflictos en curso, en el enfrentamiento ruso-ucraniano, iniciado en 2022, es público y notorio el empleo masivo de *drones* y de herramientas de IA para el reconocimiento de objetivos, además del acentuado uso de los espectros electromagnético y cibernético para acciones militares, normalmente valiéndose de tecnologías innovadoras.

En el conflicto en Franja de Gaza, iniciado en 2023, y sus posteriores derivaciones, especialmente contra Líbano e Irán, también resulta evidente el empleo de IA para la selección de objetivos y la realización de operaciones de precisión por parte de las Fuerzas de Defensa de Israel.

Ante lo expuesto, considerando lo que ya existe en términos de disrupciones y sus respectivos empleos en las guerras más recientes, se considera viable, a continuación, realizar un ejercicio deductivo sobre los posibles impactos de las nuevas tecnologías en los conflictos bélicos futuros, como se describirá seguidamente.

Implicaciones de las nuevas tecnologías para el futuro de la guerra

Inicialmente, antes de abordar el tema central de esta etapa del texto, conviene resaltar que el sistema internacional atraviesa un período turbulento, en el cual las “convergencias tecnológicas”⁷ tienden a jerarquizar a los Estados en razón de sus capacidades para dominar nuevas tecnologías.

⁷ Como se lee en Gonçalves y Macário (2026, traducción propia), “Se trata de la maduración simultánea de capas interdependientes: hardware avanzado, conectividad, inteligencia artificial, datos, sensores, energía y software, que, cuando se integran, habilitan aplicaciones híbridas e inéditas, inviables mediante una evolución aislada. Cuando estas capas ‘encajan’, el resultado no es incremental: constituye un cambio de nivel. El elemento decisivo de la convergencia es la sincronía. Las tecnologías que evolucionan fuera de ritmo tienden a generar ineficiencias sistémicas: la inteligencia artificial sin una infraestructura computacional adecuada posee un alcance limitado; la conectividad sin aplicaciones orientadas a datos se vuelve subutilizada; y los sensores sin integración analítica producen volumen, no inteligencia. La ‘convergencia’ ocurre cuando estas capas avanzan conjuntamente y pasan a operar como un sistema único, capaz de aprender, escalar y adaptarse continuamente”.

Un ejemplo de tal estratificación puede leerse en Gonçalves y Macário (2026), de la siguiente manera: los **“Desarrolladores de Tecnologías Completas (Full Stacks)”**, es decir, las potencias que dominan integralmente las plataformas, los datos de gobernanza y coordinan la investigación, la producción industrial, el financiamiento, la regulación y la estandarización de las plataformas, exportando dependencia e influyendo en la geopolítica mundial; los **“Proveedores Sofisticados”**, países con excelencia en componentes y nichos críticos (materiales, manufactura avanzada, componentes específicos e ingeniería de punta), todos integrados en cadenas globales, pero sin control total de la arquitectura de los sistemas; y las **“Colonias Digitales”**, meros consumidores de sistemas controlados por otros actores.

Asimismo, se considera inexcusable retomar la premisa de este trabajo para enfatizar que la guerra es la continuación de la política, una disputa entre voluntades antagónicas. Y, en un enfrentamiento político, es presumible que el actor “A” intente imponer su voluntad al actor “B”, y viceversa. De ahí surge la siguiente cuestión: ¿qué impulsa la voluntad del actor político?

Para responder a tal inquietud, se tomará como base el pensamiento cratológico desarrollado en la Escuela Superior de Guerra de Brasil (ESG) a lo largo de más de siete décadas. Según el pensamiento de la ESG, los Estados son animados por una fuerza denominada “Poder Nacional”⁸. Ese poder es fruto de un sistema de engranajes (didácticamente denominados “expresiones del poder”) que se mueven de manera interdependiente y generan la fuerza motriz que impulsa al ente político a alcanzar sus objetivos y le posibilita imponer su voluntad frente al actor que se le oponga.

Estos párrafos preliminares tienen por propósito apoyar el argumento de que las innovaciones disruptivas para empleo militar son consecuencia del desarrollo del poder del actor político, en la totalidad de sus expresiones, e influyen, en gran medida, en el equilibrio de poder entre las naciones, es decir, en la geopolítica mundial.

⁸ Se lee en la Escuela Superior de Guerra (2024, p. 26, traducción propia) que el Poder Nacional “es la capacidad que posee el conjunto de los hombres y de los medios que constituyen la Nación, actuando de conformidad con la voluntad nacional, para alcanzar y mantener los objetivos nacionales. Se manifiesta en cinco expresiones: la política, la económica, la psicosocial, la militar y la científica y tecnológica”.

Pasando al asunto propiamente dicho, se resalta que las innovaciones disruptivas surgen, *a priori*, en el contexto de la expresión científico-tecnológica del Poder Nacional. Sin embargo, para que la ciencia avance, es necesario que el complejo psicosocial proporcione recursos humanos capacitados y motivados para la investigación, en busca de las deseadas innovaciones. Las investigaciones, a su vez, son fomentadas por el aporte financiero derivado de una economía pujante, que permita el surgimiento de un sector productivo competente y audaz, con fuerza necesaria para conferir materialidad a las ideas gestadas en los centros de excelencia y experimentadas en los laboratorios. Y todo ello deriva de una voluntad política que defina adecuadamente los objetivos y metas que deben ser alcanzados por la sociedad y, de ser necesario, fomente su consecución.

Sin embargo, curiosamente, es en el ámbito militar, donde desembocan los resultados de todas las demás expresiones, resaltándose, una vez más, la sustantiva dependencia de recursos humanos capaces de utilizar las innovaciones disruptivas con destreza y eficiencia en el campo de batalla, siempre que ello sea necesario.

Se llama la atención del lector sobre el hecho de que el componente "recursos humanos" ha sido reiteradamente subrayado en los párrafos anteriores. Ello se debe a que no es posible innovar sin capacitar a las personas. Son los individuos, debidamente dotados de un elevado nivel de escolaridad y adecuadamente motivados para la investigación, quienes constituyen los vectores de concepción de las tecnologías disruptivas. Y, como ya se ha subrayado, esto no sucede de la noche a la mañana. Es el resultado de un proyecto que se extiende a largo plazo e involucra generaciones.

Dicho esto, del análisis de la sección anterior se deduce que las tecnologías disruptivas que tienden a impactar los conflictos bélicos del futuro son aquellas integradas a la IA. En las guerras recientes, las innovaciones empleadas están, en la mayoría de los casos, acopladas a herramientas de IA. Y es lícito suponer que tal práctica se multiplicará de aquí en adelante.

Asimismo, se prevé que los robots *serán* ampliamente utilizados para tareas específicas de desminado, apoyo logístico y otras misiones que impliquen elevada precisión, alto riesgo de bajas y/o esfuerzo repetitivo.

Además, los vehículos no tripulados, en todos los dominios, integrados con IA y dotados de LAWS – a pesar de las intensas polémicas que rodean su empleo –, desempeñarán, según todos los indicios, un papel destacado en los campos de batalla del futuro.

También se vislumbra que el empleo de la nanotecnología y de la biotecnología se ampliará a corto plazo, ofreciendo un considerable apoyo a la industria de defensa y a la medicina militar.

No obstante, las disputas por el dominio del espacio y del ciberespacio, según indican las tendencias, deberán intensificarse en un futuro próximo. Las estructuras organizacionales de las fuerzas armadas de algunos países ya contemplan comandos propios para dichos dominios⁹. Y se prevé que ello se convertirá en una práctica común, tal como ocurrió con el surgimiento de las fuerzas aéreas en el siglo XX¹⁰.

Sin embargo, para que todo ello se materialice, se considera que el dominio de la computación cuántica para el desarrollo de herramientas de IA cada vez más poderosas será un objetivo perseguido por las principales potencias militares del planeta. De manera semejante, el desarrollo y el uso de satélites como armas destructoras de satélites parecen constituir un camino sin retorno.

Conclusiones

Como resultado de los argumentos y análisis desarrollados a lo largo de estos escritos, se constata que las tecnologías disruptivas están redefiniendo el futuro de la guerra, otorgando ventajas a los países que invierten en innovación e integración de la ciencia y la tecnología en sus instrumentos de defensa.

En el transcurso del texto, se definió como premisa el pensamiento “clausewitziano” de comprensión de la guerra como la continuación de la acción política. Y, siendo así, se argumentó acerca del recurrente equívoco derivado del uso

⁹ Véanse los ejemplos de los EE.UU., mencionados en Donald Trump (2019), así como los de Brasil, expuestos en Vianna y Camelo (2020) y Brasil (2020, pp. 46-47).

¹⁰ Véase el modelo de creación de la Fuerza Aérea Brasileña, conforme se describe en FAB (2026).

inadvertido del sustantivo “guerra”, al margen de la Polemología y de las tradiciones históricas. Tal práctica genera imprecisión conceptual y provoca consecuencias indeseables para el orden interno de los Estados y para el sistema internacional en su conjunto.

Asimismo, fueron enumeradas las tecnologías disruptivas más relevantes en los conflictos bélicos recientes, a saber: la IA, los vehículos no tripulados (se llamados *dron* o no), la robotización, la cibernética, los sistemas autónomos (en especial las LAWS y la polémica que rodea su empleo, principalmente en los campos de la ética y del derecho), los satélites y los distintos medios espaciales, así como la nanotecnología y la biotecnología.

Cabe subrayar que tales innovaciones en el campo de batalla caracterizan el “principio de guerra de la sorpresa”¹¹ y, frente a las sorpresas derivadas de las disrupciones, no existen planes de contingencia por parte del actor sorprendido¹².

En lo que respecta a los protagonistas de las disrupciones en el ámbito militar, por más polémica que pueda resultar el asertividad en este tema —debido a cuestiones metodológicas y al acceso a bases de datos para su medición—, es lícito admitir que pueden considerarse como países *Full Stacks* los EE.UU. (probablemente el más robusto de todos), la República Popular China, Rusia y, quizás, Francia. Otras naciones citadas a lo largo del texto, como por ejemplo

¹¹ Según consta en Brasil (2015, p. 223, traducción propia), los Principios de la Guerra son “preceptos filosóficos derivados de estudios de campañas militares a lo largo de la historia y presentan variaciones en el espacio y en el tiempo. Constituyen puntos de referencia que orientan y respaldan a los jefes militares en la planificación y conducción de la guerra, sin, no obstante, condicionar sus decisiones”.

¹² Cabe señalar que en Brasil (2015, pp. 220-223, traducción propia) se encuentran enumerados 12 Principios de la Guerra: economía de fuerzas o de medios; explotación; maniobra; masa ofensiva; prontitud; seguridad; simplicidad; objetivo; unidad de mando; moral; y sorpresa. Este último “consiste en golpear al enemigo donde, cuando o de tal manera que no se encuentre preparado. El comandante que obtiene el efecto de sorpresa podrá alterar a su favor, de forma decisiva, la correlación de fuerzas en combate. Este principio sugiere que los esfuerzos deben emprenderse de manera tal que sorprendan al enemigo y eviten ser sorprendidos por él. Mediante el empleo de la sorpresa, podrán obtenerse resultados superiores al esfuerzo realizado, compensando factores desfavorables. La sorpresa debe ser buscada en los niveles estratégico, operacional y táctico. Se manifiesta mediante la originalidad, la audacia en las acciones, el sigilo, el engaño, la innovación tecnológica y, sobre todo, la velocidad de ejecución de las acciones y la disimulación” (énfasis nuestros).

Israel, India, Turquía e Irán, conforman un grupo de Estados que persiguen un lugar destacado en este ámbito, pero que aún pueden ser encuadrados como “Proveedores Sofisticados”. No obstante, no existen dudas de que otros Estados desarrollados, de acuerdo con los criterios adoptados, también merecen el mismo encuadramiento¹³.

No obstante, se constata que el dominio de estas tecnologías es estratégico y tiende a acentuar la asimetría entre las potencias más desarrolladas y los países con menor nivel de desarrollo, con especial relevancia para las denominadas “Colonias Digitales”. Sin embargo, por más paradójico que parezca, las disrupciones pueden favorecer a actores “menos favorecidos”, dando lugar al fenómeno de la “asimetría inversa”.

Asimismo, fue expuesto el constructo según el cual el Poder Nacional impulsa el ímpetu de los Estados hacia sus objetivos, subrayándose la relevancia de la expresión psicosocial —especialmente de los recursos humanos de la sociedad— para la obtención de tecnologías disruptivas, desde su concepción hasta su empleo en los campos de batalla.

Por último, se destaca que el fenómeno sociológico de la guerra ha mantenido sus características, pese a los avances tecnológicos. Lo que se transforma en este arte es la forma de combatir. Las tecnologías modifican las técnicas, las tácticas y los procedimientos operacionales, pero la esencia de la lucha entre voluntades, en continuidad con el enfrentamiento político, permanece inalterada.

Se concluye, pues, este trabajo transcribiendo la reflexión de un conocido filósofo israelí acerca del futuro de la humanidad frente a la evolución de la IA, pensamiento que se muestra plenamente aplicable a la evolución del arte de la guerra e induce a una profunda reflexión sobre los impactos de las disrupciones tecnológicas actualmente experimentadas:

13 Con el uso de herramientas de inteligencia artificial, fue posible obtener un ranking de países según los tres criterios de desarrollo tecnológico en el ámbito militar y, curiosamente, se obtuvieron los siguientes datos: Full Stacks – Estados Unidos, China, Rusia, Israel y Corea del Sur; y Proveedores Sofisticados – Francia, Reino Unido, Alemania, Turquía, India e Irán (nota del autor).

La sabiduría es mucho más antigua que la historia humana. Es elemental, el fundamento de la vida orgánica. Los primeros organismos no fueron creados por algún genio o dios infalible. Surgieron mediante un intrincado proceso de ensayo y error. A lo largo de 4 mil millones de años, mecanismos cada vez más complejos de mutación y autocorrección condujeron a la evolución de árboles, dinosaurios, selvas y, finalmente, seres humanos. Ahora convocamos una extraña inteligencia inorgánica que puede escapar a nuestro control y poner en riesgo no solo a nuestra especie, sino también a innumerables otras formas de vida. **Las decisiones que todos tomemos en los próximos años determinarán si la convocatoria de esta extraña inteligencia se revelará como un error terminal o como el inicio de un nuevo y prometedor capítulo en la evolución de la vida**" (Harari, 2024, Epílogo, traducción propia y énfasis nuestros).

Referencias

- Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation.
- Brasil. Ministério da Defesa (2020). *Livro branco de defesa nacional*. https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/livro_branco/Versaodolivroemporugues2020.pdf
- Brasil. Ministério da Defesa (2025). *Base industrial de defesa (BID)*. <https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/base-industrial-de-defesa/projetos-estrategicos>
- Brasil. Ministério da Defesa (2015). *Glossário das Forças Armadas: MD35-G-01* (5ª ed.). <https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf/view>
- Clausewitz, C. (1984). *On war*. EGN.
- Crevelde, M. Van (2016). *More on war*. Oxford University Press.
- Escola Superior de Guerra (2024). *Fundamentos do poder nacional*. Editora ESG.
- Força Aérea Brasileira (2026). *Atlas histórico do Brasil*. <https://atlas.fgv.br/verbe-te/8823>
- Fayal, R. A. de A., & Freire, R. R. (2024). Revisão conceitual da guerra nos tempos de hoje. In A. Santos et al. (Orgs.), *O mundo em guerra* (pp. 39-66). Processo.

- Federação das Indústrias do Estado do Rio Grande do Sul (2020). *A indústria de defesa da França*.
- Foucault, M. (2012). *Em defesa da sociedade*. WMF Martins Fontes.
- Friede, R. (2010). Guerra assimétrica reversa. *Dossiê UNESP*, 2(29), pp. 158-172. <https://doi.org/10.1590/S0101-90742010000200009>
- Gavião, L. O., & Kostin, S. (2024). Tecnologias disruptivas do mundo em guerra. In A. Santos et al. (Orgs.), *O mundo em guerra* (pp. 111–145). Processo.
- Gonçalves, A. C., & Macário, L. (2026). *Convergência tecnológica: O novo vetor de poder no século XXI*. Prospectare.
- Harari, Y. N. (2024). *Nexus: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial*. Companhia das Letras.
- Keegan, J. (2006). *Uma história de guerra*. Letras.
- Kon, A. (2020). O futuro do mundo do trabalho: Impactos do novo paradigma tecnológico. In *Cadernos Adenauer XXI*.
- Organização para Cooperação e Desenvolvimento Econômico. (2005). *Oslo manual: Guidelines for collecting and interpreting innovation data*.
- Paul, T. V. (1994). *Asymmetric conflicts: War initiation by weak powers*. Cambridge University Press.
- Rajagopalan, R. P., & Stroikos, D. (2024). A transformação da política espacial da Índia. *Space Policy*, 69, pp. 1-9. <https://doi.org/10.1016/j.space-pol.2024.101633>
- Saint-Pierre, H. L. (2013). Defesa ou segurança? In E. Mei & H. L. Saint-Pierre (Orgs.), *Paz e guerra: Defesa e segurança entre as nações* (pp. 11–37). UNESP.
- Schmitt, C. (2008). *O conceito do político e teoria do partisan*. Del Rey.
- Schwab, K. (2016). *A quarta revolução industrial*. Edipro.
- Spahr, T. W. (2024). *Raven sentry: Employing AI for indications and warnings in Afghanistan*. <https://publications.armywarcollege.edu/DesktopModules/ArticleCS/Print.aspx?PortalId=121&ModuleId=63268&Article=3789950>
- Toffler, A. (1981). *A terceira onda* (32.ª ed.). Record.
- Agência Brasil. (2019). *Trump lança comando espacial dos EUA: Meta é manter domínio americano na última fronteira militar*. <https://agenciabrasil.ebc.com.br/internacional/noticia/2019-08/trump-lanca-comando-espacial-dos-eua>

Vianna, E. W., & Camelo, J. R. S. (2020). Defesa cibernética no Brasil. *Revista da Escola Superior de Guerra*, 35(75), pp. 127-154.

Whiteman, W. E. (1998). *Training and education Army officers for the 21st century*.
<http://www.dtic.mil/dtic/tr/fulltext/u2/a345812.pdf>

CAPÍTULO SEGUNDO

BRASIL, ESCOLA SUPERIOR DE DEFESA

Competências e produção do conhecimento no campo dos estudos de defesa: a inteligência artificial generativa como paradigma educativo

Patrícia Pontes Bezerra

Aline Barbosa Xavier Muniz

Eduardo Amadeu Dutra Moresi

Resumo: Este capítulo discute as competências docentes para produção do conhecimento no campo dos Estudos de Defesa tendo a Inteligência Artificial Generativa (IAGen) como paradigma educativo. Parte do pressuposto de que a IAGen é uma tecnologia cognitiva que reorganiza práticas pedagógicas, formas de mediação docente e processos de produção do conhecimento. Aborda o debate a partir dos conceitos apresentados pela Teoria do Conhecimento Tecnológico Pedagógico do Conteúdo (TPACK). O texto analisa as especificidades do ensino de defesa, marcado por temas como segurança nacional, soberania, estratégia, defesa cibernética, inteligência, geopolítica e políticas públicas, argumentando que tais características exigem competências docentes específicas. Propõe a discussão a partir de uma abordagem baseada em revisão integrativa da literatura e análise documental, articulando estudos sobre competências, produção do conhecimento e ensino de defesa mediados pela IAGen. Como contribuição, o capítulo propõe eixos orientadores para o desenvolvimento das escolas de defesa no que tange ao processo de ensino nos Estudos de Defesa. Conclui-se que as Escolas e Colégios destinados ao ensino de defesa possuem papel fundamental para que a IAGen seja incorporada aos processos educativos preservando a autonomia humana.

Palavras-chave: competências, inteligência artificial generativa, estudos de Defesa, paradigma educacional, análise bibliométrica.

Sobre os autores: **Patricia Pontes Bezerra** é doutora em Estudos Marítimos. Chefe da Divisão Pedagógica da Escola Superior de Defesa e docente do Curso de Pós-Graduação *Lato sensu* em Ensino Militar na Universidade da Força Aérea. Desenvolve pesquisas em competências, Inteligência Artificial e ensino de Defesa. Membro dos Laboratórios de Segurança, Desenvolvimento e Defesa (SDD)/ESD e de Simulação e Cenários/UNIFA.

Aline Barbosa Xavier Muniz é doutoranda em Educação pela Universidade Católica de Brasília, Bolsista do Programa de Doutorado no Exterior da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), sendo realizado na Universidade de Aveiro, Portugal. Pedagoga da Escola Superior de Defesa. Membro do Laboratório de Segurança, Desenvolvimento e Defesa - Lab/SDD/ESD.

Eduardo Amadeu Dutra Moresi é doutor em Ciência da Informação e professor permanente dos Programas Stricto Sensu de Mestrado e Doutorado em Educação e de Mestrado Profissional em Governança, Tecnologia e Inovação da Universidade Católica de Brasília. Desenvolve pesquisas sobre o uso da Inteligência Artificial para apoiar pesquisas científicas e a escrita acadêmica.

Introdução

O campo dos Estudos de Defesa ocupa lugar estratégico na produção de conhecimentos relacionados à soberania, à segurança nacional e à compreensão das transformações tecnológicas em nível internacional. Nesse contexto, as escolas e colégios de Defesa assumem papel relevante como espaços de formação, pesquisa e integração entre civis e militares, especialmente por lidarem com processos decisórios marcados pela complexidade, pela incerteza e pela sensibilidade institucional.

O problema que orienta este capítulo consiste em compreender como se constituem as competências docentes necessárias à produção do conhecimento no campo dos Estudos de Defesa, tendo a IAGen como paradigma educativo. O objetivo geral do capítulo é analisar as competências docentes requeridas para a produção do conhecimento em Defesa em um cenário no qual a IAGen passa a operar como tecnologia cognitiva e paradigma educativo. De modo específico, busca discutir a IAGen como elemento de transformação pedagógica, examinar sua relação com a Teoria do Conhecimento Tecnológico Pedagógico do Conteúdo (TPACK), identificar tendências presentes na produção científica e eviden-

ciar lacunas que dificultam a construção de uma abordagem integrada para a formação de docentes e instrutores nesse campo.

O capítulo se apoia em uma abordagem bibliométrica qualitativa, articulada à revisão integrativa da literatura e à análise documental. A pesquisa bibliométrica foi realizada na base Scopus, inicialmente por meio de uma expressão de busca ampla envolvendo competências docentes, estudos de Defesa, inteligência artificial generativa e paradigma educativo. Como a busca integrada não retornou resultados, a estratégia foi desmembrada em expressões parciais, o que permitiu recuperar literaturas correlatas e organizar o corpus em categorias temáticas.

Como resultado, o capítulo evidencia que a literatura apresenta avanços relevantes, mas ainda fragmentados. Embora existam estudos sobre IA na educação, formação docente, competências digitais, educação militar e segurança tecnológica, ainda são escassas as pesquisas que integram essas dimensões em um mesmo quadro teórico-metodológico.

Competências docentes: o papel da Escola Superior de Defesa nos Estudos de Defesa

O conhecimento produzido no campo dos Estudos de Defesa é um ativo importante para um estado que deseja manter e desenvolver sua soberania no cenário mundial. As escolas e colégios de Defesa são, nesse sentido, um *locus* significativo para que, intencionalmente, a atividade de produção de conhecimento de Defesa encontre profissionais, métodos, estrutura física e interações sociais que promovam as aprendizagens necessárias a saberes tão diferenciados e transversais.

O advento da Inteligência Artificial representa um componente ainda mais instigante a esse processo, não apenas porque acelera a velocidade de circulação de dados e, portanto, da base do conhecimento, mas pelo potencial de transformação disruptiva que carrega nas relações entre aquele que aprende e aquele que ensina, alunos e professores. Não se trata, assim, de mais uma tecnologia incremental, mas uma mudança de paradigma educacional.

Dessa maneira, o capítulo que ora se inicia proporcionará a reflexão sobre a relação existente entre as competências docentes e a IAGen como paradigma educativo, ao considerar o campo do Ensino nos Estudos de Defesa. Tais categorias foram selecionadas por serem consideradas essenciais na contemporaneidade, mas também em uma visão prospectiva, exercício vital ao ambiente escolar. O docente e suas competências e a IAGen em seus aspectos educacionais são apresentados de maneira a criar sinergia e potencialidades, em uma visão crítica, sustentada por arcabouço teórico como também pela prática dos autores.

O novo paradigma surge, segundo Vargas (2020), como uma resposta à crise da “ciência normal” e do modelo newtoniano-cartesiano, que influenciou a educação por séculos com uma visão fragmentada, técnica e mecanizada. Enquanto o modelo antigo focava na transmissão de saberes de um professor detentor do conhecimento para um aluno passivo, o novo modelo é central na aprendizagem e no desenvolvimento de competências.

A transformação na maneira como ocorre a interação com o conhecimento caracteriza o novo paradigma como construtivista, interacionista, sociocultural e transcendente. Sob essa ótica o conhecimento não é uma verdade única e absoluta, mas composto por “teorias transitórias” que se aproximam da realidade plural.

O foco central do novo paradigma é o “aprender a aprender”, capacitando o indivíduo a tomar consciência do que sabe e a dispor-se a buscar novas informações e mudar seus próprios conceitos diante da evolução constante da sociedade.

A escola desempenha um papel importante nesse quadro, na medida em que segundo Nóvoa (1992) trata-se de um espaço central, pensado e organizado para que as aprendizagens ocorram, indo além da simples transmissão de conteúdo. Para o autor a escola não é uma organização onde há “aplicação” de técnicas produzidas fora dela, mas sim como um lugar de reflexão sobre as práticas, reservando para isto uma especial atenção às funções desempenhadas pelos professores, considerados profissionais produtores de saber e saber-fazer.

Isso significa que a mudança educacional e a inovação não ocorrem isoladamente no professor, mas dependem de uma transformação na organização escolar e no seu funcionamento, sendo um contexto no qual trabalhar e formar não são atividades distintas, mas promova um elo entre a teoria acadêmica e a realidade social.

A formação de professores deve ser concebida como uma das componentes da mudança, em conexão estreita com outros sectores e áreas de intervenção, e não como uma espécie de condição prévia da mudança. A formação não se faz antes da mudança, faz-se durante, produz-se nesse esforço de inovação e de procura dos melhores percursos para a transformação da escola. (Nóvoa, 1992, p. 17)

Nesse contexto o conceito de Competências emerge das novas demandas educacionais geradas aos professores e alunos no que tange à perspectiva do “que e como” deve ser ensinado. Segundo Ramos (2001) o conceito surge atendendo a três propósitos:

a) reordenar conceitualmente a relação trabalho-educação, desviando o foco dos empregos, das ocupações e das tarefas para o trabalhador em suas implicações subjetivas com o trabalho; b) institucionalizar novas formas de educar/formar os trabalhadores e gerir o trabalho internamente às organizações e no mercado de trabalho em geral, sob novos códigos profissionais em que figuram as relações contratuais, de carreira e de salário; c) formular padrões de identificação da capacidade real do trabalhador para determinada ocupação (...). (Ramos, 2001, p. 39)

A autora destaca, ainda, que restringir a noção de competência, cuja origem remonta aos trabalhos McClelland (1973), à mudança da lógica da qualificação taylorista-fordista, estática e fragmentada do mundo do trabalho para um dinamismo e subjetividade do trabalhador formado é uma simplificação que não assimila a complementariedade dos processos anteriores.

Cabe destacar que a incorporação do conceito de competências não ocorreu de maneira homogênea, sendo marcada por estudos da década de 1990 pelos estudos de Prahalad e Hamel (1990) e outros estudiosos do tema, resultando três grandes matrizes, conforme apresentado por Bezerra e Muniz (2024): a matriz condutivista baseada na psicologia comportamental, percebendo as competên-

cias como características de fundo do indivíduo que causam um desempenho eficaz; a matriz funcionalista, cuja base teórica emprega a teoria dos sistemas, utilizando a análise funcional para construir competências partindo das funções gerais para as específicas; e a matriz construtivista, segundo as autoras mais aderente ao campo da educação, tendo em vista que busca unir as necessidades da organização às percepções dos trabalhadores, valorizando a aprendizagem individual e coletiva.

As autoras analisam o marco regulatório brasileiro no que tange às competências na Política Nacional de Desenvolvimento de Pessoas (PNDP - Decreto nº 9.991/2019), alterado pelo Decreto nº 10.560/2020, a qual busca induzir a excelência dos órgãos públicos por meio da identificação de “lacunas de competência”.

Bezerra e Muniz (2024) destacam, ainda, que a Gestão por Competências não é um movimento linear, mas um Processo “em Espiral”, no qual as competências institucionais, missão e visão de futuro, precisam estar alinhadas às competências individuais. Tais reflexões permitem inferir às várias interfaces do processo de ensino e desenvolvimento de competências. No caso do objeto do presente capítulo, a complexidade do ensino no campo dos Estudos de Defesa.

O conceito de estudos de defesa é apresentado por Medeiros (2015) como um campo de conhecimento interdisciplinar e em constante evolução, que ultrapassa as nomenclaturas tradicionais e as definições normativas rígidas. A autora argumenta que os estudos de defesa são marcados por uma forte interdisciplinaridade, envolvendo a combinação de teoria política, relações internacionais e sociologia com métodos e objetos da economia, administração e estudo de conflitos. Introduz a hipótese dos “campos híbridos”, sugerindo que a área é mais ampla do que as definições normativas no Brasil costumam abrigar, integrando regiões interdisciplinares diversas. Observa que o campo é frequentemente identificado por nomenclaturas mais antigas, como ciências militares, estudos militares ou estudos estratégicos. Enquanto os estudos estratégicos tradicionalmente centralizavam no binômio guerra e paz, a pesquisa em defesa moderna expandiu-se para incluir temas como gestão de recursos, tecnologia dual e ilícitos transnacionais.

O campo de estudos de defesa é, segundo Medeiros (2015) formado por elementos de ordem evolucionária, no qual a complexidade é predominante e os

sistemas se adaptam progressivamente às necessidades institucionais e conjunturais. Dessa maneira não deve haver uma perspectiva de hierarquização dos saberes, mas uma disposição em rede, organizada por “*clusters* de proximidade”. Tais *clusters* agrupam temas variados que vão desde logística e economia de defesa até segurança pública, direito internacional marinho e inovação tecnológica.

Um elemento central apresentado por Medeiros (2015) é que o campo dos estudos de defesa promove a aproximação entre o mundo civil e o militar. A autora destaca que essa interação criou uma comunidade epistêmica onde “se fizeram militares no *ethos* da Academia e civis no *ethos* dos militares”, impulsionada por políticas públicas e uma conjuntura de internacionalização.

A relação entre as competências docentes a produção do conhecimento e campo da Defesa: a IAGen como paradigma educativo recebe uma importante contribuição dos estudos de Etzkowitz e Zhou (2017): o conceito de hélice tríplice. Trata-se de um modelo de inovação no qual a universidade (academia), a indústria e o governo interagem como esferas institucionais primárias para promover o desenvolvimento por meio da inovação e do empreendedorismo. Esse modelo constitui um processo dinâmico e contínuo que visa a criação de um ecossistema de inovação, servindo como um guia para políticas e práticas nos âmbitos local, regional e nacional.

A tese da hélice tríplice sustenta que a universidade deixa de ter um papel social secundário para tornar-se uma fonte fundamental de novo conhecimento, agindo de forma integrada com o governo e a indústria para gerar crescimento econômico e desenvolvimento social. Considerando as devidas especificidades serão apresentadas reflexões acerca do papel destinado pela Escola Superior de Defesa. A análise particular dessa instituição não pretende criar generalizações, mas permitir discussões fecundas no que se relaciona a influência das novas tecnologias em cenários de operações futuras no que tange à formação por competências e ao papel do professor. Cabe salientar que Quaresma *et al.* (2024) descrevem uma evolução no para o conceito de hélice quádrupla, no qual são incorporadas a dimensão ambiental e ecológica ao processo de produção do conhecimento.

A Escola Superior de Defesa (ESD) desempenha um papel fundamental no atual Planejamento Estratégico Setorial de Defesa (PESD 2024-2035), especial-

mente na integração entre civis e militares e ao desenvolvimento de tecnologias disruptivas, como a inteligência artificial (IA).

O cenário estratégico para 2024-2035 define que o Setor de Defesa deve estimular atividades de pesquisa e desenvolvimento em tecnologias disruptivas, citando explicitamente a inteligência artificial, além de computação quântica e sistemas não tripulados. A ESD está inserida no esforço de obter e manter o domínio dessas tecnologias de interesse da defesa, como instituição de Ciência e Tecnologia do Ministério da Defesa.

Um dos objetivos estratégicos apresentados pelo documento é consolidar a ESD como referência na promoção de estudos de defesa no âmbito da sociedade civil. No cenário da IA, isso implica que a escola deverá: promover a inserção da temática de defesa no sistema de educação nacional, atraindo o meio acadêmico para o debate sobre como a IA impacta a soberania nacional, formando pesquisadores civis e capacitando lideranças da sociedade e servidores de diversos ministérios nos temas de defesa, o que inclui o entendimento das novas ameaças e oportunidades cibernéticas e tecnológicas. O PESD estabelece como uma de suas ações setoriais de defesa: "Estimular, no âmbito do Setor de Defesa, as atividades de pesquisa e desenvolvimento em tecnologias disruptivas como a inteligência artificial, a realidade virtual e aumentada, a computação quântica e os sistemas não tripulados, dentre outros." (Brasil, p. 26 e 27).

Portanto, é possível identificar a atuação da ESD como parte do esforço para aperfeiçoar a integração entre governo, indústria e academia (hélice tríplice). A escola serve como um elo para: incentivar a produção de pesquisas científicas e a realização de eventos que discutam tecnologias de interesse da defesa; fomentar a interação entre o seu próprio sistema de ensino e os das Forças Armadas e da Escola Superior de Guerra (ESG); e contribuir. (Brasil, p. 25).

Dessa maneira a ESD é instada a apoiar transversalmente o Objetivo Nacional de Defesa de promover a autonomia tecnológica, embora os setores estratégicos (nuclear, cibernético e espacial) tenham coordenações específicas nas Forças Singulares. O domínio da IA é visto como um fator que acentua, nesse cenário, as assimetrias na área da Defesa e, nesse sentido, a capacitação de recursos humanos de alto nível pela ESD é essencial para que o Brasil não exerça um papel secundário no cenário mundial.

Cabe destacar que o reconhecimento do referencial teórico e normativo que oferece suporte às atividades e ao cumprimento da missão da ESD impulsionou ações recentes voltadas ao desenvolvimento de competências em Inteligência Artificial Generativa (IAGen) entre os docentes. Nesse contexto, foi criado, em 2024, um Grupo de Trabalho multidisciplinar com a finalidade de implementar a Inteligência Artificial na ESD; foram realizadas, em anos consecutivos, três semanas pedagógicas destinadas à capacitação docente, dedicadas à temática da Inteligência Artificial; além da promoção de oficinas inicialmente direcionadas aos docentes e, posteriormente, aos discentes, de modo a fomentar uma massa crítica sobre o tema.

As reflexões apresentadas permitem compreender que as escolas e colégios de Defesa possuem no contexto da Defesa um papel importante como *cluster* de conhecimento no que se refere à inovação e, no tempo presente à IAGen, atuando por meio das suas competências institucionais e de seus docentes componentes. No caso específico do Brasil ainda existem lacunas, algumas delas apresentadas a seguir, que precisam ser identificadas, sendo objeto de ação sistematizada no ambiente estratégico e escolar.

Inteligência artificial generativa como paradigma educativo

Ao identificar da IAGen como paradigma educativo nos estudos de defesa, apresenta-se a tese de que o uso da IAGen nos processos educativos pode coexistir desde que a ética, pensamento crítico e centralidade humana estejam consolidadas nas estratégias metodológicas. Esse paradigma rejeita dois extremos: a IAGen como solução aos problemas educacionais e a exclusão total da IAGen no contexto da produção do conhecimento nos estudos de defesa.

Neste sentido, a inteligência artificial pode ser considerada um paradigma educacional no campo dos estudos de defesa, apoiada pela teoria de Kuhn, (1998), a medida em que altera o modo como uma comunidade científica formula problemas, interpreta evidências, define métodos, constrói o conhecimento e disponibiliza à sociedade, por meio da escrita científica. Dessa forma, a IAGen pode ser defendida como paradigma educacional nos estudos de defesa a partir de cinco deslocamentos principais. Primeiro, desloca o ensino, da transmissão de conteúdo para a formulação crítica de problemas. Segundo, desloca a

aprendizagem, da memorização para a validação, curadoria e argumentação. Terceiro, desloca a avaliação, do produto para o acompanhamento do processo cognitivo. Quarto, desloca a escrita científica de uma prática exclusivamente humana para uma prática humano-IAGen. Quinto, desloca o papel docente de expositor para mediador epistemológico.

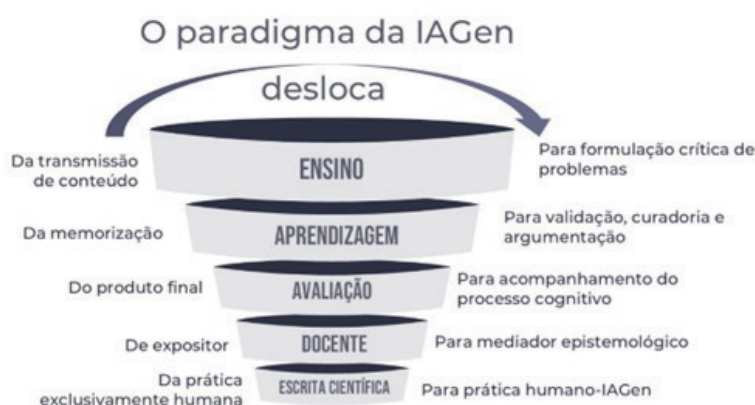


Figura 1. Deslocamentos dos processos educativos. Fonte: elaborada pelos autores.

Nesse paradigma, o valor pedagógico da IAGen se distancia de um gerador de conteúdo e aproxima de uma ampliação da capacidade humana de formular problemas, testar hipóteses, validar informações, reconhecer vieses, preservar a autoria humana e produzir conhecimento responsável em contextos marcados por incerteza, complexidade e sensibilidade estratégica.

No campo da educação superior, O'Dea (2024) apresenta a discussão da IAGen como uma mudança paradigmática. A autora situa a IAGen como uma força que impacta ensino, aprendizagem, avaliação e pesquisa, porque ferramentas generativas passaram a ser amplamente utilizadas por estudantes e professores, essa dimensão estrutural de mudança de paradigma afeta a organização do trabalho acadêmico e pode redefinir propostas de aprendizagem.

No campo dos estudos de defesa, essa mudança paradigmática é acrescida pela especificidade da formação, pois os temas estratégicos como segurança nacional, soberania, ameaças híbridas, geopolítica, defesa cibernética, inteligência, fronteiras, guerra informacional e tomada de decisão sob incerteza re-

vela uma nova ecologia de formação em que professores e estudantes precisam aprender a interagir criticamente com sistemas generativos, avaliando outputs, identificando viés, nivelando o risco e analisando as implicações dentro do campo de estudo. E para isto é preciso repensar a formação docente a partir de uma teoria que sustente essa diversidade que é a Teoria do conhecimento tecnológico pedagógico do conteúdo.

As teorias pedagógicas: TPACK

Em uma instituição de ensino superior voltada à formação em alto nível, a integração da IAGen nas práticas pedagógicas é fundamental para a internalização dessas tecnologias nos processos educativos, concebidas de forma transversal e não compartimentada. Nesse contexto, a Teoria do Conhecimento Tecnológico Pedagógico de Conteúdo (TPACK), derivada da proposta de Shulman (1986), que é a Teoria do conhecimento pedagógico do conteúdo (PCK) sobre a articulação entre conhecimento de conteúdo (CK), conhecimento pedagógico (PK). Neste aspecto o conhecimento tecnológico (TK), é inserido da tríade, compondo a tríade no processo de ensino. A figura 2 representa a interseção entre esses conhecimentos.

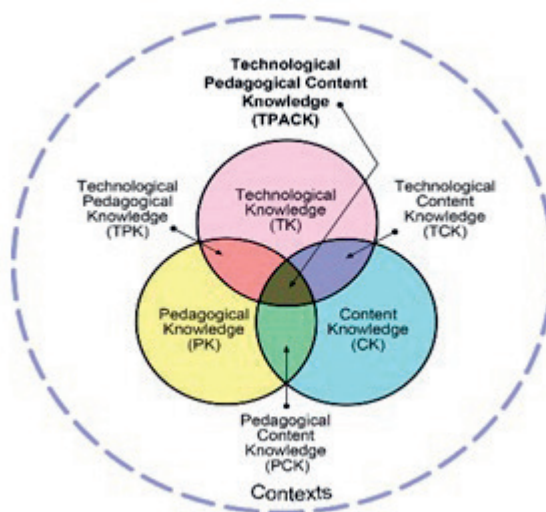


Figura 2. Representação do TPACK. Fonte: (Koehler & Mishra, 2009).

Shulman (1986) discute a natureza do ensinar, a formação do professor e o paralelo com outras profissões, como engenharia, medicina e o clero ao contestar a máxima atribuída a George Bernard Shaw *He who can, does. He who cannot, teaches*, que poder ser traduzido por “Quem sabe faz. Quem não sabe, ensina”. Posteriormente, Koehler e Mishra, (2009) ampliaram essa fundamentação ao incorporar o componente tecnológico, formalizando o quadro TPACK que representa o ponto de encontro entre saber técnico do conteúdo, saber pedagógico e o saber tecnológico na prática docente.

Gonzales *et al.* (2025) sustentam, entretanto, que as dimensões clássicas do TPACK não capturam plenamente a complexidade da adoção de IAGen, recomendando o alargamento AI-TPACK e a verificação de quanto o conhecimento docente prevê integração pedagógica significativa. Na pesquisa com docentes, Tan, Cheng e Ling (2025) identificaram que a competência em IA prediz TPACK, e que TPACK, por sua vez, prediz o desempenho docente, ou seja, o efeito da competência em IA sobre desempenho é indireto.

Celik (2026) propõe o *Intelligent-TPACK*, no qual incide a avaliação ética do professor sobre o uso da IA como elemento norteador para ações de capacitação, implementação e direcionamentos da IA na educação.

IAGen como objeto, meio e ambiente de formação

A TPACK-AI nos estudos de Defesa pode assumir três dimensões na formação de professores e instrutores. A primeira é o conhecimento estratégico do conteúdo e está relacionado ao domínio dos conceitos e problemas próprios da Defesa com a mediação de problemas incertos, controversos e interdisciplinares. A segunda dimensão é o conhecimento tecnológico generativo. Envolve compreender como modelos generativos funcionam, quais são seus limites e como interagir com eles por meio de uma comunicação eficaz, sendo necessário, ainda, avaliar vieses, alucinações, autoria, integridade acadêmica, proteção de dados e confiabilidade das fontes. A terceira dimensão é a do conhecimento pedagógico estratégico com IA no campo da Defesa, de modo a apoiar atividades de ensino, como produção de questões problematizadoras, elaboração de roteiros de simulação e na construção de cenários.

Neste sentido, o uso pedagógico deve ser orientado por intencionalidade docente, sendo necessárias capacitações que abordem o letramento e didática e avaliação com IA (Prilop *et al.*, 2025). Essa dimensão é sensível, pois a produção do conhecimento no campo da Defesa envolve interpretação de ameaças, análise de capacidades, leitura de cenários, formulação de hipóteses e responsabilidade sobre decisões. Corresponde à capacidade de desenhar situações de aprendizagem em que a IAGen contribua para ampliar a análise crítica sem substituir o julgamento humano, dentro dos processos de ensino, aprendizagem, avaliação e produção de escrita científica.

A partir do TPACK e de suas ampliações para a IAGen, é possível propor uma nova configuração adaptada à realidade nos estudos de Defesa, apresentado na figura 3.



Figura 3. Estrutura de conhecimento com IAGen nos estudos de Defesa. Fonte: elaborada pelos autores.

Essa estrutura de conhecimento com IAGen no campo da defesa possui uma saída que são processos educativos que alinham competências e promovem caminhos de formações para docentes e instrutores das Escolas de Defesa inserindo o aspecto do conhecimento tecnológico e pedagógico alinhados as estratégias com uso da IAGen.

Metodologia da pesquisa na base Scopus

A análise bibliométrica foi empregada para a análise do objetivo deste capítulo, realizada por meio de uma pesquisa na base Scopus, para recuperar os meta-

dados de publicações científicas sobre o tema. Foi elaborada a expressão de busca: ("teacher competenc*" OR "teaching competenc*" OR "faculty competenc*" OR "educator competenc*" OR "teacher professional development" OR "faculty development" OR "teacher education" OR "teacher training" OR "instructor training") AND ("defense education" OR "defence education" OR "defense studies" OR "defence studies" OR "military education" OR "professional

Bloco	Expressão de Busca	Descrição
1	("teacher competenc*" OR "teaching competenc*" OR "faculty competenc*" OR "educator competenc*" OR "teacher professional development" OR "faculty development" OR "teacher education" OR "teacher training" OR "instructor training")	Contempla o eixo central da pesquisa: a formação, o desenvolvimento profissional e as competências necessárias ao exercício da docência. Inclui diferentes denominações usadas na literatura internacional para tratar professores, docentes universitários, educadores e instrutores. Sua função é recuperar estudos que abordem tanto competências propriamente ditas quanto processos formativos, capacitação, educação docente e desenvolvimento profissional, permitindo analisar como essas competências são constituídas e aprimoradas.
2	("defense education" OR "defence education" OR "defense studies" OR "defence studies" OR "military education" OR "professional military education" OR "strategic studies" OR "security studies" OR "military instructor*")	Delimita o contexto específico da investigação: a educação, os estudos e a produção do conhecimento no campo da Defesa. Abrange termos relacionados à educação militar, estudos de defesa, estudos estratégicos, segurança e formação de instrutores militares. Sua função é direcionar a busca para produções que discutam práticas educacionais, formação profissional e desenvolvimento acadêmico em ambientes civis e militares vinculados à Defesa.
3	("generative artificial intelligence" OR "generative AI" OR GenAI OR ChatGPT OR "large language model*" OR LLM)	Insere a inteligência artificial generativa como elemento tecnológico e epistemológico da pesquisa. Abrange termos associados à IAGen, aos modelos de linguagem de grande escala e a ferramentas amplamente estudadas no contexto educacional. Sua função é recuperar estudos que discutam o impacto dessas tecnologias na docência, na aprendizagem, na pesquisa, na autoria e na produção do conhecimento.
4	("educational paradigm" OR "pedagogical paradigm" OR "teaching paradigm" OR "learning paradigm" OR "pedagogical innovation" OR "educational transformation")	qualifica a IAGen como possível fator de transformação educacional. Reúne termos relacionados a paradigmas pedagógicos, modelos de ensino e aprendizagem, inovação pedagógica e transformação educacional. Sua função é identificar estudos que tratem mudanças nas práticas docentes, nas formas de mediação pedagógica e nas concepções educacionais, superando uma abordagem meramente instrumental da tecnologia.

Quadro 1. Descrição dos blocos da expressão de busca. Fonte: elaborada pelos autores.

military education" OR "strategic studies" OR "security studies" OR "military instructor*") AND ("generative artificial intelligence" OR "generative AI" OR GenAI OR ChatGPT OR "large language model*" OR LLM) AND ("educational paradigm" OR "pedagogical paradigm" OR "teaching paradigm" OR "learning paradigm" OR "pedagogical innovation" OR "educational transformation"). O Quadro 1 apresenta a descrição de cada um dos blocos. Cabe salientar, contudo, que o resultado da pesquisa foi nulo.

A ausência de resultados na expressão completa indica que a interseção simultânea entre competências docentes, campo da Defesa, inteligência artificial generativa e paradigma educativo ainda é pouco consolidada ou não aparece indexada na Scopus com essa combinação terminológica. Por isso, o desmembramento em expressões parciais foi metodologicamente mais adequado, pois permitiu mapear literaturas correlatas que, articuladas entre si, sustentam a discussão do artigo. O Quadro 2 apresenta as expressões de busca e os quantitativos recuperados na base Scopus.

O bloco 1 - Defesa e paradigma educativo - relaciona o campo da Defesa às discussões sobre paradigmas, inovação pedagógica e transformação educacional. Seu objetivo é identificar estudos que tratem mudanças nos modelos de ensino, aprendizagem e formação em contextos de defesa, educação militar, estudos estratégicos e segurança. O segundo bloco - Defesa e inteligência artificial - articula o campo da Defesa com a inteligência artificial, incluindo IAGen, ChatGPT, modelos de linguagem e tecnologias correlatas. A ampliação do termo para "artificial intelligence" é adequada, pois parte da literatura pode tratar a IAGen dentro do campo mais amplo da IA, sem empregar termos específicos como GenAI ou LLM.

O bloco 3 - competências docentes, inteligência artificial e paradigma educativo - relaciona competências docentes, inteligência artificial/IAGen e transformação educacional. Seu foco está na literatura educacional mais ampla, buscando estudos sobre formação docente, desenvolvimento profissional e inovação pedagógica diante da emergência da IA e dos modelos generativos. O último bloco - competências docentes e campo da Defesa - aproxima o eixo das competências docentes ao campo da Defesa, contemplando estudos sobre formação de professores, instrutores, docentes universitários e profissionais envolvidos em educação militar, estudos de defesa, segurança e estratégia.

A separação em expressões parciais, permitiu recuperar produções científicas situadas em interseções temáticas menores, mas diretamente relacionadas ao tema de pesquisa. Essa estratégia permitiu recuperar 373 referências bibliográficas. Em seguida foi aplicado o filtro para delimitar os tipos de documentos em artigos de periódicos, de revisão e de anais de congressos, além de livros e de capítulos de livros.

A Tabela 1 apresenta os principais indicadores bibliométricos do corpus analisado, composto por 361 documentos publicados entre 1985 e 2026. A Figura 1

Bloco	Expressão de Busca	Quant
1. Defesa e paradigma educativo	("defense education" OR "defence education" OR "defense studies" OR "defence studies" OR "military education" OR "professional military education" OR "strategic studies" OR "security studies" OR "military instructor*") AND ("educational paradigm" OR "pedagogical paradigm" OR "teaching paradigm" OR "learning paradigm" OR "pedagogical innovation" OR "educational transformation")	5
2. Defesa e inteligência artificial	("defense education" OR "defence education" OR "defense studies" OR "defence studies" OR "military education" OR "professional military education" OR "strategic studies" OR "security studies" OR "military instructor*") AND ("artificial intelligence" OR "generative AI" OR GenAI OR ChatGPT OR "large language model*" OR LLM OR "generative pre-trained transformer*")	149
3. Competências docentes, inteligência artificial e paradigma educativo	("teacher competenc*" OR "teaching competenc*" OR "faculty competenc*" OR "educator competenc*" OR "teacher professional development" OR "faculty development" OR "teacher education" OR "teacher training" OR "instructor training") AND ("artificial intelligence" OR "generative AI" OR GenAI OR ChatGPT OR "large language model*" OR LLM OR "generative pre-trained transformer*") AND ("educational paradigm" OR "pedagogical paradigm" OR "teaching paradigm" OR "learning paradigm" OR "pedagogical innovation" OR "educational transformation")	194
4. Competências docentes e estudos de defesa	("teacher competenc*" OR "teaching competenc*" OR "faculty competenc*" OR "educator competenc*" OR "teacher professional development" OR "faculty development" OR "teacher education" OR "teacher training" OR "instructor training") AND ("defense education" OR "defence education" OR "defense studies" OR "defence studies" OR "military education" OR "professional military education" OR "strategic studies" OR "security studies" OR "military instructor*")	25

Quadro 2. Expressões parciais e os quantitativos recuperados na base.Ç Scopus.
Fonte: elaborada pelos autores.

apresenta a evolução temporal. Embora o intervalo temporal cubra mais de quatro décadas, a idade média dos documentos, de 2,91 anos, evidencia a concentração recente da produção científica, indicando que o tema tem recebido atenção crescente nos últimos anos. Esse padrão é reforçado pela taxa anual de crescimento de 10,68%, valor que sugere uma área em expansão e com aumento expressivo de interesse acadêmico. A presença de registros referentes a 2026 indica a inclusão de documentos em pré-publicação ou de acesso antecipado, o que reforça o caráter contemporâneo e emergente do campo investigado.

Descrição	Resultados
Período	1985:2026
Fontes (Periódicos, Anais, Livros, etc)	288
Documentos	361
Taxa de Crescimento Anual %	10,68
Idade média do documento	2,91
Média de citações por documento	7,803
Referências	23057
Palavras-chave Plus (ID)	1496
Palavras-chave dos Autores (DE)	1084
Autores	990
Autores de documentos com um único autor	85
Colaboração de Autores	
Documentos com um único autor	97
Coautores por documento	2,91
Coautorias internacionais %	18,84
Tipos de Documentos	
artigos	176
livros	33
capítulos de livros	44
artigo de conferência	84
artigo de revisão	24

Tabela 1. Principais indicadores sobre o Corpus. Fonte: elaborada pelos autores.

Os dados também revelam elevada dispersão das publicações, uma vez que os 361 documentos estão distribuídos em 288 fontes distintas. Essa relação próxi-

ma entre número de documentos e número de fontes sugere um campo ainda fragmentado, sem a predominância clara de periódicos ou canais editoriais centrais. Tal característica é comum em áreas emergentes ou interdisciplinares, nas quais a produção científica tende a circular por diferentes espaços de publicação, incluindo periódicos multidisciplinares, anais de conferências, livros e capítulos.

Em relação à autoria, observa-se a participação de 990 autores, com média de 2,91 coautores por documento, indicando um padrão moderado de colaboração científica. A taxa de coautoria internacional, correspondente a 18,84% e demonstra a existência de articulações transnacionais, embora ainda em nível relativamente limitado quando comparado a campos fortemente internacionalizados. Além disso, a presença de 97 documentos de autoria individual, aproximadamente 27% do corpus, evidencia que contribuições autorais individuais continuam desempenhando papel relevante na consolidação teórica e conceitual da área.

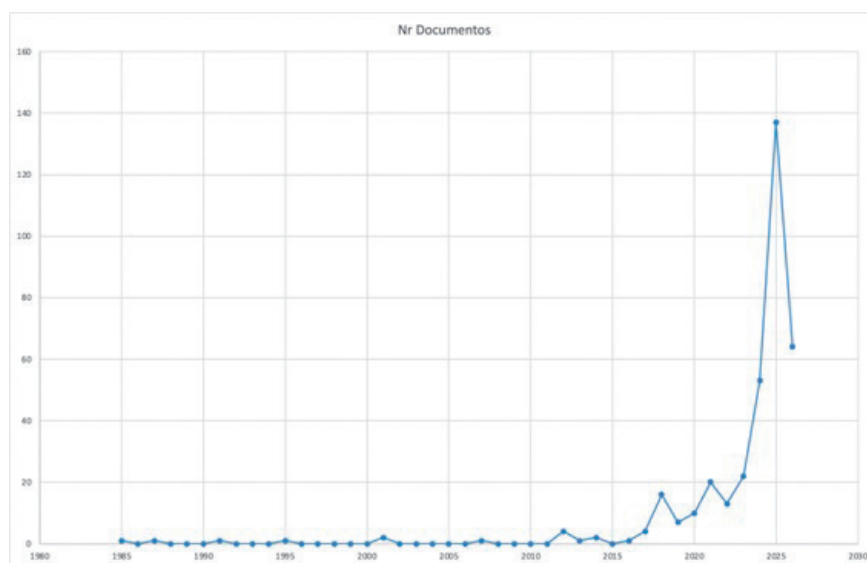


Figura 4. Evolução das publicações no período de 1985 a 2026. Fonte: elaborada pelos autores.

Quanto ao impacto acadêmico, a média de 7,803 citações por documento deve ser interpretada à luz da baixa idade média das publicações. Considerando que grande parte da produção é recente, esse índice sugere uma recepção inicial

consistente e potencial de crescimento do impacto científico ao longo do tempo. O corpus reúne ainda 23.057 referências, o que corresponde a uma média aproximada de 63 referências por documento. Esse dado indica elevada densidade referencial e sugere que os estudos analisados se apoiam em uma base teórica ampla, possivelmente oriunda de diferentes tradições disciplinares.

Por fim, a distribuição dos tipos documentais revela uma configuração híbrida da comunicação científica no campo. A predominância de artigos científicos, acompanhada por expressiva presença de trabalhos de conferência, livros e capítulos, indica que a área combina canais típicos de disseminação rápida do conhecimento com formatos mais extensos e analíticos. Esse padrão sugere uma interface entre campos de rápida atualização, como áreas tecnológicas e aplicadas, e tradições acadêmicas das Ciências Sociais e Humanidades, nas quais livros e capítulos mantêm relevância significativa para o desenvolvimento de argumentos teóricos mais aprofundados.

Resultados da pesquisa

A presente seção aprofunda a interpretação qualitativa das categorias temáticas identificadas, a partir da análise semântica dos títulos e resumos dos documentos que compõem o corpus bibliográfico da pesquisa. Essa etapa teve como objetivo compreender de que modo os diferentes agrupamentos bibliográficos contribuem para a delimitação do campo investigativo sobre competências docentes para produção do conhecimento no campo da Defesa, tendo a Inteligência Artificial Generativa como paradigma educativo.

O agrupamento em cinco categorias permitiu organizar a produção científica em macroeixos temáticos que expressam diferentes dimensões do objeto investigado. Esses eixos abrangem: a aplicação da Inteligência Artificial à inovação pedagógica e à aprendizagem personalizada; o desenvolvimento de competências docentes, literacia em IA, ChatGPT e TPACK; a educação militar, a formação de instrutores e a produção do conhecimento em Defesa; a relação entre IA, segurança, guerra, estratégia e governança tecnológica; e, por fim, a segurança técnica dos sistemas de IA, a ciberdefesa e a defesa algorítmica. Essa organização favorece uma leitura integrada do corpus, ao evidenciar que o tema da pesquisa não se situa em uma única tradição disciplinar, mas emerge

da interseção entre educação, tecnologia, formação docente, estudos estratégicos, segurança e Defesa.

A compreensão de cada categoria foi orientada pelo objetivo geral da pesquisa, considerando a IAGen como paradigma educativo. Nesse sentido, a análise não se limitou a indicar a frequência ou a centralidade dos documentos, mas a interpretação de como cada agrupamento contribuiu para a delimitação teórica, metodológica e epistemológica do tema. Os artigos mais relevantes de cada categoria foram considerados em função de sua proximidade semântica com o centro do respectivo agrupamento, permitindo identificar tendências, recorrências conceituais e possíveis articulações entre os campos da educação, da Inteligência Artificial e da Defesa.

Essa etapa assume particular importância porque a literatura analisada revelou um campo ainda em processo de consolidação. Embora existam estudos consolidados sobre IA na educação, competências digitais docentes, formação de professores, IA militar, segurança tecnológica e educação militar, ainda são escassas as abordagens que integram esses temas em torno da constituição de competências docentes para produção do conhecimento em Defesa com apoio da IAGen.

A seguir, são apresentadas as análises das cinco categorias temáticas resultantes do agrupamento semântico, destacando seus principais conteúdos, sua relação com o problema de pesquisa e sua contribuição para a construção de uma agenda científica sobre competências docentes, IAGen e produção do conhecimento no campo da Defesa.

IA educacional, inovação pedagógica e aprendizagem personalizada

A primeira categoria reúne estudos que tratam da Inteligência Artificial como vetor de inovação pedagógica, personalização da aprendizagem, avaliação adaptativa, tutoria inteligente, inclusão educacional e incorporação de tecnologias emergentes aos processos formativos. Esses trabalhos indicam que a IA vem sendo progressivamente associada à reorganização dos ambientes de ensino e aprendizagem, especialmente por sua capacidade de apoiar feedbacks individualizados, experiências educacionais adaptativas, recursos de realidade

aumentada, gamificação, acompanhamento do desempenho discente e ampliação das possibilidades de inclusão educacional (Belmaadadia & Meliani, 2026; Kaviyaraj & Uma, 2021; Lafham & Bachari, 2025; Mantilla-Sánchez *et al.*, 2026; Martín-Rodríguez & Madrigal-Cerezo, 2025; Mohamad *et al.*, 2025; Ramos Piñas *et al.*, 2026; Salendab *et al.*, 2025; Singh *et al.*, 2026; Tohănean *et al.*, 2025).

No contexto desta pesquisa, essa categoria permite compreender a IAGen como parte de uma transformação educacional mais ampla, na qual o professor deixa de ser concebido apenas como transmissor de conteúdo e passa a exercer funções mais complexas, como designer pedagógico, mediador tecnológico, curador de informações e avaliador crítico de ambientes inteligentes de aprendizagem.

No campo da Defesa, a IAGen pode apoiar a construção de cenários, simulações, estudos de caso, exercícios de decisão, análise documental e personalização de trajetórias formativas. Entretanto, sua apropriação exige competências docentes específicas, capazes de integrar recursos inteligentes a objetivos formativos complexos.

Competências docentes, ChatGPT, literacia em IA e TPACK

A segunda categoria constitui o núcleo mais diretamente associado ao objetivo geral da pesquisa, pois reúne estudos sobre formação docente, competências digitais, uso do ChatGPT, literacia em IA, TPACK, prontidão para inovação, desenvolvimento profissional e transformação das práticas pedagógicas. Os documentos analisados indicam que a competência docente na era da IAGen envolve a articulação entre conhecimento pedagógico, conhecimento tecnológico, domínio do conteúdo, pensamento crítico, reflexão profissional e capacidade de avaliar a pertinência epistemológica dos resultados produzidos por sistemas generativos (Abykenova *et al.*, 2026; Ayanwale *et al.*, 2025; Kohnke, 2025; Liang *et al.*, 2025; Martínez *et al.*, 2025; Novoa-Echaurren *et al.*, 2025; Onbasili, 2026; Romero García *et al.*, 2025; Urazbayeva *et al.*, 2024; Wang *et al.*, 2025).

A IAGen pode apoiar a elaboração de planos de aula, a síntese de literatura, a construção de exercícios, a geração de cenários e a revisão de textos científicos. Contudo, também pode produzir respostas imprecisas, enviesadas, incom-

pletas ou inadequadas a contextos sensíveis. Por essa razão, a competência docente exige validação crítica, curadoria qualificada, problematização dos resultados e explicitação dos critérios de uso da IA. Nessa direção, modelos como o TPACK podem ser ampliados para incorporar dimensões próprias do campo da Defesa.

Educação militar, formação de instrutores e produção do conhecimento em Defesa

A terceira categoria aproxima o corpus bibliográfico do campo específico da Defesa, reunindo documentos sobre educação militar, formação de instrutores, educação para defesa nacional, pensamento estratégico, liderança, tradição intelectual em Defesa e produção do conhecimento em ambientes militares. A formação nesse campo envolve cultura profissional, hierarquia, doutrina, responsabilidade pública, ética, liderança, análise histórica, tomada de decisão e interpretação de conflitos (de Santis, 2026; Howard, 2018a, 2018b, 2018c, 2018d; Huang *et al.*, 2012; Otřísal & Loyka, 2025; *Research anthology on military and defense applications, utilization, education, and ethic*, 2021; Wu & Huang, 2012; Wu *et al.*, 2012).

Os estudos sobre formação militar, educação para defesa nacional, pensamento crítico em educação militar profissional e formação de professores para contextos de Defesa indicam que o docente desse campo atua como mediador entre conhecimento acadêmico, prática profissional e demandas institucionais. A presença de textos associados à tradição estratégica, especialmente aqueles vinculados a Michael Howard (2018), reforça a centralidade da história, da prudência analítica e da interpretação contextual para a produção do conhecimento em Defesa.

Nesse sentido, a IAGen deve ser integrada ao ensino de Defesa sem empobrecer a densidade intelectual do campo. A competência docente em Defesa deve, portanto, ser compreendida como uma competência de mediação entre tradição estratégica, inovação pedagógica, rigor epistemológico e responsabilidade institucional. Essa categoria sugere que as reflexões aqui apresentadas possam trazer contribuições ao explicitar como a IAGen reconfigura, mas não eli-

mina, o papel formativo do professor na produção de conhecimento sensível e aplicado à Defesa.

IA, segurança, guerra, estratégia e governança tecnológica

A quarta categoria concentra estudos que articulam Inteligência Artificial, segurança nacional, guerra futura, competição estratégica, ciberpoder, regulação, operações informacionais, estabilidade internacional e governança tecnológica. Os estudos analisados indicam que a IA já integra debates sobre guerra algorítmica, influência informacional, inovação em Defesa, segurança humana, regulação, ciberoperações, guerra centrada em redes e competição entre grandes potências (Baker, 2024; Bommakanti, 2025; Chen, 2024; Çitak, 2024; Hunter *et al.*, 2024; Johnson, 2021; Raska & Bitzinger, 2023; Sanclemente, 2022; Sharma, 2024; Sinozic-Martinez & Jahnel, 2024).

A literatura demonstra que o professor de Defesa precisa compreender a IA não apenas como ferramenta didática, mas também como objeto de estudo, instrumento de poder e fator de transformação da segurança internacional. O docente que utiliza IAGen na produção do conhecimento em Defesa precisa formar estudantes capazes de analisar operações informacionais, vieses cognitivos, confiabilidade dos sistemas de IA, governança de tecnologias emergentes e implicações éticas da automação militar.

Além disso, essa categoria sugere que a IAGen pode contribuir para atividades de cenarização, análise prospectiva, síntese de literatura estratégica e formulação de problemas de pesquisa, desde que acompanhada por validação crítica e controle epistemológico. A competência docente, nesse caso, não se limita à fluência digital. Ela envolve julgamento estratégico, consciência normativa, análise de riscos e compreensão do papel da tecnologia na transformação da guerra, da segurança e da governança internacional.

Segurança técnica de sistemas de IA, ciberdefesa e defesa algorítmica

A quinta categoria reúne estudos de natureza mais técnica, voltados à segurança de sistemas inteligentes, ataques adversários, envenenamento de dados,

redes neurais, *deep learning*, detecção de ameaças, cibersegurança, robustez algorítmica e defesa de sistemas autônomos. Embora essa categoria não se concentre diretamente na formação docente, ela é indispensável para o tema da pesquisa porque explicita uma dimensão frequentemente negligenciada nos debates educacionais sobre IAGen: a vulnerabilidade técnica dos sistemas de IA (Abtahi *et al.*, 2026; Cao *et al.*, 2022; Gao *et al.*, 2024; Kim & Jung, 2021; Kim *et al.*, 2021; Liu *et al.*, 2018; Qiang *et al.*, 2021; Samonte *et al.*, 2024; Shibly *et al.*, 2022; Xie *et al.*, 2022).

Os trabalhos agrupados demonstram que modelos inteligentes podem ser expostos a ataques, manipulações, erros de classificação, infecções neurais, perturbações adversariais e falhas de segurança. Tais vulnerabilidades têm implicações diretas para contextos de Defesa, nos quais a confiabilidade informacional, a segurança dos dados e a integridade dos sistemas são condições fundamentais para a produção e o uso responsável do conhecimento.

Para a constituição de competências docentes no campo da Defesa, essa categoria sugere que o professor precisa desenvolver uma literacia crítica sobre segurança algorítmica. Isso implica reconhecer que a IAGen não é neutra, infalível ou tecnicamente estável. Em contextos militares e de segurança, esses cuidados são ainda mais relevantes, pois erros informacionais podem produzir consequências institucionais e estratégicas.

Principais achados das categorias temáticas

A análise das cinco categorias temáticas evidencia que a produção científica sobre competências docentes para a produção do conhecimento no campo da Defesa, tendo a Inteligência Artificial Generativa como paradigma educativo, ainda se configura como um campo emergente, interdisciplinar e em processo de consolidação. O corpus analisado demonstra que há literatura consistente sobre Inteligência Artificial na educação, formação docente, competências digitais, educação militar, IA aplicada à segurança e defesa algorítmica; contudo, esses temas aparecem de forma fragmentada. O principal achado, portanto, é que o objeto desta pesquisa se situa em uma zona de convergência entre campos ainda pouco integrados.

A primeira categoria, voltada à IA educacional, inovação pedagógica e aprendizagem personalizada, demonstra que a Inteligência Artificial vem sendo incorporada aos processos educacionais como recurso para personalização, avaliação adaptativa, tutoria inteligente, inclusão, gamificação e apoio ao engajamento discente. No entanto, também revela que sua adoção exige planejamento pedagógico, avaliação crítica e adequação ao contexto escolar.

A segunda categoria, referente às competências docentes, ChatGPT, literacia em IA e TPACK, constitui o núcleo mais diretamente relacionado ao objetivo da pesquisa. Os estudos agrupados mostram que a competência docente na era da IAGen não se reduz ao domínio técnico de ferramentas digitais. No campo da Defesa, essa competência assume maior complexidade, pois deve incorporar segurança informacional, sigilo, confiabilidade, doutrina, responsabilidade ética e tomada de decisão sob incerteza.

A terceira categoria, centrada na educação militar, formação de instrutores e produção do conhecimento em Defesa, evidencia que a docência nesse campo possui especificidades institucionais, epistemológicas e profissionais. A tecnologia pode apoiar a produção acadêmica, a análise documental e a elaboração de cenários, mas não substitui o julgamento estratégico, histórico e ético do docente. Assim, a competência docente em Defesa deve ser entendida como uma competência de mediação entre tradição profissional, inovação pedagógica e responsabilidade institucional.

A quarta categoria, relativa à IA, segurança, guerra, estratégia e governança tecnológica, amplia o entendimento da IAGen para além do campo educacional. Portanto, o docente precisa formar estudantes capazes de compreender a IA como tecnologia de poder, instrumento de transformação da guerra e fator de reconfiguração da segurança internacional. A competência docente, nesse caso, exige julgamento estratégico, consciência normativa, análise de riscos e compreensão crítica das implicações políticas e éticas da IA.

A quinta categoria, dedicada à segurança técnica de sistemas de IA, ciberdefesa e defesa algorítmica, evidencia uma dimensão frequentemente pouco explorada nas discussões pedagógicas: a vulnerabilidade técnica dos sistemas inteligentes. O docente precisa compreender que sistemas generativos não são neutros, infalíveis ou plenamente seguros. Por isso, a literacia em IA, no contexto da Defesa, deve incluir também uma literacia sobre segurança algorítmica.

As competências docentes necessárias à produção do conhecimento no campo da Defesa com apoio da IAGen são multidimensionais, elas envolvem competências pedagógicas, tecnológicas, informacionais, éticas, estratégicas, institucionais e securitárias. Desse modo, o principal achado integrador é que a IAGen deve ser compreendida como um paradigma educativo em construção, capaz de transformar práticas docentes, processos formativos e dinâmicas de investigação.

A contribuição potencial da pesquisa está em propor uma leitura integrada dessas dimensões, aproximando literaturas que, embora relacionadas, ainda aparecem dispersas: IA educacional, formação docente, competências digitais, educação militar, estudos de Defesa, segurança internacional e defesa algorítmica.

Quanto às lacunas científicas, a análise das cinco categorias temáticas evidencia que a literatura sobre Inteligência Artificial, formação docente, educação militar, segurança e Defesa apresenta avanços relevantes, mas ainda de forma fragmentada em relação ao problema central desta pesquisa: **de que maneira são constituídas as competências docentes para a produção do conhecimento no campo da Defesa, tendo a Inteligência Artificial Generativa como paradigma educativo**. O principal *gap* científico identificado é a inexistência de uma abordagem integrada que articule, em um mesmo quadro teórico-metodológico, competências docentes, IAGen, produção do conhecimento, educação militar, segurança informacional, governança tecnológica e epistemologia da Defesa.

Conclusão

Este capítulo discutiu como se constituem as competências docentes necessárias à produção do conhecimento no campo dos Estudos de Defesa, considerando a Inteligência Artificial Generativa como paradigma educativo. A análise evidenciou que a IAGen não altera apenas o uso de ferramentas digitais, mas reorganiza práticas de ensino, mediação docente, escrita científica e validação do conhecimento. No campo da Defesa, essa transformação exige atenção especial ao rigor científico, à autonomia humana, à segurança informacional, à ética e à responsabilidade institucional.

Os resultados indicam que a literatura apresenta avanços importantes, porém ainda fragmentados. Há estudos sobre IA na educação, formação docente, competências digitais, educação militar e segurança tecnológica, mas ainda são escassas as abordagens que integram essas dimensões em um modelo específico para o campo da Defesa. Assim, a principal lacuna identificada está na ausência de um quadro de competências docentes capaz de articular o uso pedagógico da IAGen às exigências epistemológicas, estratégicas e institucionais desse campo.

As competências docentes no campo da Defesa devem ser compreendidas como uma construção multidimensional, que transcende o domínio técnico da Inteligência Artificial Generativa (IAGen) e envolve a capacidade de utilizá-la de forma crítica, ética e contextualizada. Isso implica não apenas saber operar ferramentas de IAGen, mas também reconhecer seus limites, validar informações, preservar a autoria intelectual humana e interpretar criticamente os resultados produzidos pela tecnologia.

Nessa perspectiva, a IAGen pode constituir-se em importante potencializadora da produção do conhecimento, desde que seu uso seja orientado por intencionalidade pedagógica, critérios de confiabilidade e responsabilidade ética. Mais do que uma inovação instrumental, trata-se de uma tecnologia que desafia docentes e instituições a redefinirem práticas de ensino, pesquisa e produção científica.

Assim, as escolas e colégios de Defesa assumem papel estratégico ao favorecer o desenvolvimento de modelos formativos, pesquisas empíricas com docentes civis e militares e protocolos institucionais voltados ao uso seguro, crítico, transparente e pedagogicamente orientado da IAGen. Ao promover tais iniciativas, essas instituições poderão contribuir não apenas para a qualificação das competências docentes, mas também para o fortalecimento de uma cultura acadêmica comprometida com a integridade científica, a inovação responsável e a formação de profissionais capazes de atuar criticamente diante dos desafios contemporâneos da Defesa.

Referências

- Abtahi, F., Seoane, F., Pau, I., & Vega-Barbas, M. (2026). Data poisoning vulnerabilities across health care artificial intelligence architectures: Analytical security framework and defense strategies. *Journal of Medical Internet Research*, 28 (1), Article e87969. <https://doi.org/10.2196/87969>
- Abykenova, D., Assainova, A., Abildinova, G., & Kanaibekova, G. (2026). Profile of an AI-era teacher: Research on the relationship between digital competence and readiness for technological innovation. *Frontiers in Education*, 11, Article 1770448. <https://doi.org/10.3389/feduc.2026.1770448>
- Ayanwale, M. A., Adelana, O. P., Bamiro, N. B., Olatunbosun, S. O., Idowu, K. O., & Adewale, K. A. (2025). Large language models and GenAI in education: Insights from Nigerian in-service teachers through a hybrid ANN-PLS-SEM approach. *F1000Research*, 14, Article 258. <https://doi.org/10.12688/f1000research.161637.1>
- Baker, J. E. (2024). Promise and peril: The next ten years of national security AI and its regulation. In *International security studies and technology: Approaches, assessments, and frontiers*. <https://doi.org/10.4337/9781035336241.00018>
- Belmaadadia, I., & Meliani, M. (2026). Inclusive pedagogy and artificial intelligence in the teaching of physical education and sports. In *Transforming humanities and social sciences through AI*. <https://doi.org/10.4018/979-8-3373-3436-3.ch012>
- Bezerra, P. P., & Muniz, A. B. X. (2024). Explorando a evolução do conceito de competências: Da teoria à prática. In V. M. Caminha & C. P. Nascimento (Orgs.), *Abordagens em segurança, desenvolvimento e defesa: A pesquisa no LAB-SDD* (pp. 83-101). <https://encurtador.com.br/EVTi>
- Bommakanti, K. (2025). *India and network-centric warfare: The importance of cyber, electronic warfare and space technologies*. Routledge. <https://doi.org/10.4324/9781003650089>
- Brasil. (2019). *Decreto nº 9.991, de 28 de agosto de 2019*. Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da administração pública federal direta, autárquica e fundacional. Presidência da República. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9991.htm
- Brasil. Ministério da Defesa. (2024). *Planejamento Estratégico Setorial de Defesa: PESD 2024-2035*. <https://www.gov.br/defesa/pt-br/aceso-a-informacao/governanca/governanca-do-setor-de-defesa/planejamento-estrategico-1/arquivos/2025/pesd-versao-de-diagramacao-final.pdf>

- Cao, J., Jiang, L., & Lin, Z. (2022). Research on detection and defense methods of adversarial samples. In *EEL 2022: 4th International Conference on Electronic Engineering and Informatics*. <https://www.scopus.com/pages/publications/85166394886?origin=resultslist>
- Celik, I. (2026). Teachers' professional knowledge to prevent students' overreliance on AI: Insight from Intelligent-TPACK. In *Innovations in Education and Teaching International*. Routledge. <https://doi.org/10.1080/14703297.2026.2663355>
- Chen, J. Q. (2024). Teaching next-generation cyber warfare. In *European Conference on Information Warfare and Security, ECCWS*. <https://doi.org/10.34190/eccws.23.1.2436>
- Çitak, E. (2024). Current technological trends and developments in the field of security. In *Cyber security in the age of artificial intelligence and autonomous weapons*. <https://doi.org/10.1201/9781003441700-2>
- De Santis, I. (2026). Critical thinking applied to leadership and professional military education. In *Advancing military practice through military humanities*. <https://doi.org/10.4324/9781003738886-4>
- Etzkowitz, H., & Zhou, C. (2017). Hélice Triíplice: inovação e empreendedorismo universidade-indústria-governo. *Estudos Avançados*, 31(90), 23-48. <https://doi.org/10.1590/s0103-40142017.3190003>
- Gao, X., Jin, X., Miao, S., Jiang, Q., Dong, Y., Zhou, W., & Yao, S. (2024). A security study of multimodel artificial intelligence system: Adaptive retention attack for object detection system with multifocus image fusion. *Advanced Intelligent Systems*. <https://doi.org/10.1002/aisy.202300771>
- Gonzales, J. D. R., Reyna, J. T., Pajuelo, J. I. T., Gomez, R. J. M., & Zavaleta, A. R. S. (2025). Analyzing TPACK and Demographic Influences on Faculty Adoption of ChatGPT in Latin American Higher Education. *International Journal of Learning, Teaching and Educational Research*, 24(7), 402-424. <https://doi.org/10.26803/ijlter.24.7.20>
- Howard, M. (2018a). Are we at war? (2008). *Adelphi Series*, 58(472-474), 367-378. <https://doi.org/10.1080/19445571.2018.1721803>
- Howard, M. (2018b). Deterrence, consensus and reassurance in the defence of Europe (1983). *Adelphi Series*, 58(472-474). <https://doi.org/10.1080/19445571.2018.1721792>
- Howard, M. (2018c). Lessons of the Cold War (1994). *Adelphi Series*, 58(472-474), 341-350. <https://doi.org/10.1080/19445571.2018.1721800>

- Howard, M. (2018d). When are wars decisive? (1999). *Adelphi Series*, 58 (pp. 472-474), 351–366. <https://doi.org/10.1080/19445571.2018.1721802>
- Huang, M.-C., Wu, C.-Y., & Tzeng, J.-R. (2012). Sophistication of Taiwan high school military training and education system of teacher education research. *Advanced Materials Research*, 393-395, 288–291. <https://doi.org/10.4028/www.scientific.net/AMR.393-395.288>
- Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: How the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. *Defense and Security Analysis*, 40 (2), pp. 235–269. <https://doi.org/10.1080/14751798.2024.2321736>
- Johnson, J. (2021). *Artificial intelligence and the future of warfare: The USA, China, and strategic stability*. Manchester University Press. <https://doi.org/10.7765/9781526145062>
- Kaviyaraj, R., & Uma, M. (2021). A survey on future of augmented reality with AI in education. In *Proceedings of the International Conference on Artificial Intelligence and Smart Systems*. <https://doi.org/10.1109/ICAIS50930.2021.9395838>
- Kim, K., & Jung, I. Y. (2021). Secure object detection based on deep learning. *Journal of Information Processing Systems*, 17 (3), pp. 571–585. <https://doi.org/10.3745/JIPS.03.0161>
- Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, 103, Article 102150. <https://doi.org/10.1016/j.cose.2020.102150>
- Kuhn, T. S. (1998). *A estrutura das revoluções científicas* (5th ed., Vol. 5). Perspectiva.
- Kohnke, L. (2025). AI's transformative impact on teacher education: Enhancing in-service and preservice training. In *Handbook of artificial intelligence in higher education*. <https://doi.org/10.4337/9781035338764.00048>
- Koehler, M. J., & Mishra, P. (2009). What Is Technological Pedagogical Content Knowledge? *Contemporary Issues in Technology and Teacher Educations*, 9, pp. 60–70. <https://citejournal.org/wp-content/uploads/2016/04/v9i1general1.pdf>
- Lafham, M., & Bachari, E. E. (2025). Smart tutoring systems in Education 4.0: A systematic review. In *SITA 2025: 15th International Conference on Intelligent*

- Systems: Theories and Applications*. <https://doi.org/10.1109/SITA67914.2025.11273659>
- Liang, Y., Jin, S., Chen, T., & Li, N. (2025). Heterogeneity in AI readiness and its influence on behavioral intentions to use artificial intelligence. *Innovation in Language Learning and Teaching*. <https://doi.org/10.1080/17501229.2025.2565289>
- Liu, T., Wen, W., & Jin, Y. (2018). SIN2: Stealth infection on neural network—A low-cost agile neural Trojan attack methodology. In *Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust*. <https://doi.org/10.1109/HST.2018.8383920>
- Mantilla-Sánchez, M., Yépez-Moreno, A., & Núñez-Naranjo, A. (2026). Neuroeducation as a pillar of inclusion: The application of cognitive science in inclusive pedagogy. *Lecture Notes in Networks and Systems*. https://doi.org/10.1007/978-3-032-07992-3_4
- Martín-Rodríguez, A., & Madrigal-Cerezo, R. (2025). Technology-enhanced pedagogy in physical education: Bridging engagement, learning, and lifelong activity. *Education Sciences*, 15 (4), Article 409. <https://doi.org/10.3390/educsci15040409>
- Martínez, C. M., Roger-Monzo, V., & Castelló-Sirvent, F. (2025). Generative AI and critical thinking in online higher education: Challenges and opportunities. *RIED-Revista Iberoamericana de Educación a Distancia*, 28(2), 233–273. <https://doi.org/10.5944/ried.28.2.43556>
- Medeiros, S. E. (2015). Da epistemologia dos estudos de defesa e os seus campos híbridos. *Revista Brasileira de Estudos de Defesa*, 2(2), 43–55. <https://doi.org/10.26792/rbed.v2n2.2015.63034>
- Mohamad, A. F. B. N., Sharibudeen, N. S. B., Selvam, K. A. L., Lee, C. Y., Ahmad, S. N. B. S., Rani, N. B. A., Thiagarajam, A., & Aslam, S. (2025). Artificial intelligence in education: A tool for equity or a barrier to inclusion. *Environment and Social Psychology*, 10 (10), Article 4016. <https://doi.org/10.59429/esp.v10i10.4016>
- Nóvoa, A. (1992) *Os professores e a sua formação*. Dom Quixote.
- Novoa-Echaurren, Á., Pavez, I., & Anabalón, M. E. (2025). Reflective practice and digital technology use in a university context: A qualitative approach to transformative teaching. *Education Sciences*, 15 (6), Article 643. <https://doi.org/10.3390/educsci15060643>

- Onbasili, Ü. I. (2026). Empowering pre-service teachers with generative AI: A GenAI-TPACK-based approach to digital storytelling. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-026-13991-5>
- Otrřisal, P., & Loyka, V. (2025). Opportunities and challenges of defence education in teacher training. *Obrana a Strategie*, 25 (2), pp. 105-131. <https://doi.org/10.3849/1802-7199.25.2025.02.105-131upd>
- O'Dea, X. (2024). Generative AI: is it a paradigm shift for higher education? *Studies in Higher Education*, 49 (5), pp. 811-816. <https://doi.org/10.1080/03075079.2024.2332944>
- Prahalad, C. K., & Hamel, G. (1990). La competencia esencial de la corporación. *Harvard Business Review*, pp. 79-89. <https://doi.org/10.25100/cdea.v13i19.262>
- Prilop, C. N., Mah, D. K., Jacobsen, L. J., Hansen, R. R., Weber, K. E., & Hoya, F. (2025). Generative AI in teacher education: Educators' perceptions of transformative potentials and the triadic nature of AI literacy explored through AI-enhanced methods. *Computers and Education: Artificial Intelligence*, 9. <https://doi.org/10.1016/j.caeai.2025.100471>
- Qiang, C. Q., Ping, L. J., Gang, S., & Hui, W. Z. (2021). Ensemble method for net traffic classification based on deep learning. In *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing*. <https://doi.org/10.1109/ICCWAMTIP53232.2021.9674165>
- Quaresma, F. R. P., Santos, L. C., Pontes-Silva, A., Schott, E., Santos, L. L., & Porto Júnior, F. G. R. (2024). Modelos de hélices tripla, quádrupla e quántupla: O papel das universidades. *SciELO Preprints*. <https://doi.org/10.1590/SciELOPreprints.8086>
- Ramos, M. N. (2001). *A pedagogia das competências: autonomia ou adaptação?*. Cortez.
- Ramos Piñas, D., Castillo Rodríguez, M. N., Zevallos Guadalupe, V., & Suárez Reynoso, C. A. (2026). Educational innovation with artificial intelligence: An emerging paradigm for personalized learning. *Clío. Revista de Historia, Ciencias Humanas y Pensamiento Crítico*. <https://doi.org/10.5281/zenodo.17282108>
- Raska, M., & Bitzinger, R. A. (2023). *The AI wave in defence innovation: Assessing military artificial intelligence strategies, capabilities, and trajectories*. Routledge. <https://doi.org/10.4324/9781003218326>
- Research anthology on military and defense applications, utilization, education, and ethic*. (2021). <https://encurtador.com.br/IErA>

- Romero García, C., Buzón-García, O., & Parra González, E. (2025). Evaluation of a program to enhance online lecturers' digital competence: TPACK and artificial intelligence. *Online Learning Journal*, 29 (4), 109-132. <https://doi.org/10.24059/olj.v29i4.5016>
- Salendab, F. A., Cogo, D. A., Catipay, A. Z., & Millendez, G. T. (2025). The role of artificial intelligence (AI) in personalized learning and adaptive assessments. In *Transforming education with data science in the AI era*. <https://doi.org/10.4018/979-8-3373-2185-1.ch004>
- Samonte, M. J. C., Goc-Ong, A. E., Matoza, R. B. F., & Viernes, R. G. A. (2024). Evaluating the effectiveness of artificial intelligence in integrated system architectures to combat cybersecurity threats. In *International Conference on Computer and Communication Engineering Technology*. <https://doi.org/10.1109/CCET62233.2024.10838195>
- Sanclemente, G. L. (2022). Reliability: Understanding cognitive human bias in artificial intelligence for national security and intelligence analysis. *Security Journal*, 35 (4), pp. 1328-1348. <https://doi.org/10.1057/s41284-021-00321-2>
- Sharma, M. (2024). *Building China into a cyber superpower: Desires, drivers, and devices*. Routledge. <https://doi.org/10.4324/9781003473510>
- Shibly, K. H., Hossain, M. D., Inoue, H., Taenaka, Y., & Kadobayashi, Y. (2022). Autonomous driving model defense study on hijacking adversarial attack. *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-031-15937-4_46
- Singh, S., Dhiman, P., Bonkra, A., Al-Mousa, M. R., Rana, A. K., Giri, J., Chadge, R., & Zaid, A. A. (2026). AI and augmented reality: Revolutionizing educational approaches. *Studies in Systems, Decision and Control*. https://doi.org/10.1007/978-3-031-89771-9_104
- Sinozic-Martinez, T., & Jahnel, J. (2024). Technology assessment for human security: Aligning security cultures with human security in AI innovation. *Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, 33 (2), pp. 16-21. <https://doi.org/10.14512/tatup.33.2.16>
- Shulman, L. (1986). Those Who Understand: Knowledge Growth in Teaching. *American Educational Research Association*, 1. <https://www.wcu.edu/webfiles/pdfs/shulman.pdf>
- Tohänean, D. I., Vulpe, A. M., Mijaica, R., & Alexe, D. I. (2025). Embedding digital technologies (AI and ICT) into physical education: A systematic review of inno-

- vations, pedagogical impact, and challenges. *Applied Sciences*, 15(17), Article 9826. <https://doi.org/10.3390/app15179826>
- Urazbayeva, G., Kussainova, R., Aibergen, A., Kaliyeva, A., & Kantayeva, G. (2024). Innovation off the bat: Bridging the ChatGPT gap in digital competence among English as a foreign language teachers. *Education Sciences*, 14 (9), Article 946. <https://doi.org/10.3390/educsci14090946>
- Vargas, R. S. de, & Araújo, M. C. P. de. (2020). A construção de um novo paradigma educacional e sua relação com as tecnologias de informação e comunicação. *Revista Insignare Scientia (RIS)*, 3 (1), pp. 235–256. <https://doi.org/10.36661/2595-4520.2020v3i1.11335>
- Wang, Y., Li, Y., Zhang, M., & Liu, Y. (2025). An empirical study on how blended learning promotes the enhancement of digital application competence among pre-service teachers. In *8th International Conference on Educational Technology Management, ICETM 2025*. <https://doi.org/10.1109/ICETM67477.2025.11413479>
- Wu, C.-Y., & Huang, M.-C. (2012). A study of teacher training program for all-people-defense education in Taiwan. *ICIC Express Letters*, 6(6), pp. 1587–1591. <https://www.scopus.com/pages/publications/84859383596?origin=resultlist>
- Wu, C.-Y., Huang, H.-Y., & Huang, M.-C. (2012). The effects of the development of teachers training programs. *Advanced Materials Research*, 430-432, pp. 185–188. <https://doi.org/10.4028/www.scientific.net/AMR.430-432.185>
- Xie, Z., Xiang, Y., Li, Y., Zhao, S., Tong, E., Niu, W., Liu, J., & Wang, J. (2022). Security analysis of poisoning attacks against multi-agent reinforcement learning. *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-030-95384-3_41



CAPÍTULO TERCERO

COLOMBIA, ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”

Defensa multidominio: evolución de los sistemas de defensa multicapa en los escenarios operacionales futuros

Fabio Leonardo Caro Cancelado
Aldemar Serrano Cuervo
Jonnathan Jimenez-Reina

Resumen: Este capítulo trata sobre cómo las mutaciones de las amenazas y la transformación del entorno estratégico obligan a los Estados a pasar de la defensa antiaérea tradicional a las tecnologías de defensa multicapa enmarcadas en una verdadera doctrina de multidominio. Se establece como una revisión analítico-sintética de literatura, doctrinas y estudios estratégicos contemporáneos, articuladas con los aportes de tesis de los sistemas complejos. El estudio establece que la eficacia futura de la defensa, como un todo, tendrá que ver necesariamente con arquitecturas abiertas, interoperables, con fusión de sensores, integración de IA, ciberresiliencia, y un enlace funcional multidominio. Este capítulo se presenta como una traducción del Estado del Arte sobre IAMD y de operaciones multidominio, bajo un esquema conceptual para la evolución de la defensa multicapa, que enfatiza las necesidades de los Estados medianos.

Palabras clave: Defensa aérea y antimisil; Defensa multicapa; Estudios estratégicos de seguridad y defensa; Infraestructura crítica y ciberresiliencia; Operaciones multidominio; Sistemas complejos adaptativos.

Acerca de los autores: Fabio Leonardo Caro Cancelado, Mayor General del Ejército Nacional de Colombia. Profesional en Ciencias Militares. Especialista en Docencia Universitaria, Comando y Estado Mayor, y Seguridad y Defensa Nacionales. Magíster en Seguridad y Defensa Nacionales. Ha sido Comandante de la Séptima y Octava División, Comandante de Brigada y Director de Infantería. Cuenta con amplia experiencia en operaciones militares y numerosas condecoraciones nacionales e internacionales. Actualmente se desempeña como Director de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG Colombia).

Aldemar Serrano Cuervo (E.C.), Coronel del Ejército Nacional de Colombia, docente e investigador en Estudios Estratégicos de Seguridad y Defensa. Realizó estancia posdoctoral en Pensamiento Complejo en la Multiversidad Mundo Real Edgar Morin (México). Es Doctor en Logística y Gestión de Cadenas de Suministro por la Universidad de La Sabana; Magíster en Seguridad y Defensa Nacionales por la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG Colombia); Administrador de Empresas por la Universidad Militar Nueva Granada y Profesional en Ciencias Militares por la Escuela Militar de Cadetes "General José María Córdova". Actualmente se desempeña como Vicedirector de Investigación, Jefe del Doctorado en Estudios Estratégicos, Seguridad y Defensa y Jefe del Sello Editorial de la ESDEG Colombia.

Jonnathan Jiménez-Reina, Candidato a Doctor en Seguridad Internacional por la Universidad Nacional de Educación a Distancia (UNED) y el Instituto Universitario General Gutiérrez Mellado (España). Magíster en Seguridad y Defensa Nacionales y Magíster en Derechos Humanos y Derecho Internacional de los Conflictos Armados por la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG Colombia). Profesional en Política y Relaciones Internacionales por la Universidad Sergio Arboleda. Actualmente se desempeña como Docente Ocasional Asociado de Tiempo Completo en la ESDEG Colombia, Editor en Jefe de la revista Estudios en Seguridad y Defensa e Investigador Asociado reconocido por MinCiencias.

Introducción

Desde el inicio del siglo XXI hasta las primeras décadas de este siglo, se han registrado transformaciones profundas en el entorno estratégico internacional que han modificado la forma en que los Estados competen, intimidan y conducen una guerra. La rápida innovación tecnológica, la reconfiguración geopolítica del sistema internacional, la aparición de actores no estatales que cuentan

con acceso a tecnologías de doble uso y un aumento de la lucha que se extiende hacia los dominios no tradicionales han dado lugar a escenarios de operaciones con mayores niveles de complejidad, ambigüedad, velocidad y una mayor persistencia estratégica (Wirtz, 2019; Freedman, 2019; Serrano Cuervo, 2026a).

En tal sentido, la distinción clásica entre el concepto de guerra y el concepto de paz se ha vuelto cada vez más confusa, siendo esta competencia de hoy un enfrentamiento que, en ocasiones, se desarrolla por debajo del umbral de la guerra abierta. Es decir, a través de campañas extensivas que combinan medios políticos, económicos, tecnológicos, informacionales y militares en áreas de confrontación prologadas, ambiguas y de múltiples dominios. En tales espacios, las operaciones en zonas grises, la guerra híbrida, la coerción sistémica, la manipulación informacional, la explotación de vulnerabilidades tecnológicas y la presión sobre infraestructuras críticas son maneras comunes en el intercambio estratégico (Gray, 2015; Hoffman, 2007; Mazarr, 2015; Serrano Cuervo, 2026a). De esta manera, la cuestión crítica a solucionar de la defensa será la existencia de medios potenciadores de la fuerza y la organización de sistemas de defensa multicapa. Estos últimos deben ser capaces de repeler un ataque compuesto por un ataque aéreo y un terrestre al mismo tiempo, o uno marítimo y con vertientes provenientes del ciberespacio.

Las guerras recientes son la confirmación de esta mutación. La experiencia ucraniana determinó la centralidad de introducir drones, sensores, fuegos de precisión, sistemas de mandos y control, guerras electrónicas y la explotación de *big data* para producir efectos tácticos y operacionales de forma veloces. De forma convergente, los episodios de guerra entre Irán e Israel demostraron la importancia de las arquitecturas multicapa de defensa aérea y antimisil, la saturación por vectores combinados y la resiliencia ante las amenazas híbridas y cinético-tecnológicas concurrentes. En ambos casos, la ventaja tenía que ver con plataformas en particular y con la capacidad de articular sistemas de sistemas, mantener la coherencia decisional y proveerse de capacidades para adaptarse a ritmos operacionales cada vez más comprimidos (Fox, 2021; Fox, 2026; Gürsu, 2026; Davis, 2025; Kunertova, 2023).

A pesar de todo, estos cambios no significan que la esencia de la guerra haya cambiado. Tal y como establece la teoría clásica de la estrategia, y tal y como reitera la literatura contemporánea (bajo la idea de que “la guerra sigue siendo

un fenómeno político”), se entiende que la guerra es una lucha entre voluntades que utilizan para alcanzarlos todos aquellos instrumentos que pueden ponerlos en funcionamiento y que, para tal propósito, acuden a la violencia organizada, a la coerción e incluso a la incertidumbre (Clausewitz, 2007; Gray, 2015; Freedman, 2019; Serrano-Cuervo, 2026b; Serrano Cuervo, 2026a). Lo que sí está cambiando a fondo es su propio carácter, en lo que se considera que están cambiando los medios, los ritmos, los espacios, las vulnerabilidades, los centros de gravedad, las formas de integración entre la información, la decisión y la acción.

En este sentido, las nuevas amenazas se entienden como representaciones de lo que es una mayor transformación de conflicto contemporáneo. La inteligencia artificial, la automatización militar, el análisis masivo de datos, los sistemas autónomos, la guerra cognitiva, la dependencia tecnológica, la vulnerabilidad de las infraestructuras digitales o el desarrollo de las tecnologías cuánticas, se establecen como formas de cambio que significan conseguir ventajas tácticas (Horowitz, 2018; Scharre, 2018; Serrano Cuervo, 2026a; Serrano-Cuervo, 2026c).

Por lo anterior, la cuestión estratégica más crítica apunta a la introducción de nuevas tecnologías y a cómo éstas impactan en la misma infraestructura de conflicto y qué capacidades institucionales, doctrinales, cognitivas y operativas son precisas para poder responder a estas. Por lo cual, la cuestión de fondo se enfoca en cómo se integran las características anteriores en sistemas coherentes de decisión, mando, seguridad, aprendizaje y adaptación. Por eso, la guerra contemporánea supone un viraje desde enfoques centrados en plataformas y capacidades aisladas hacia marcos analíticos basados en sistemas de mayor complejidad, resiliencia funcional e integración multidominio (Serrano-Cuervo, 2026c; Serrano-Cuervo, 2026d).

En este punto, es preciso señalar esta realidad para Estados medianos y en contextos como el colombiano o el latinoamericano, donde los actores armados no estatales confluyen con economías ilícitas, el acceso a tecnologías, las vulnerabilidades institucionales y las luchas por el control de un espacio físico, y también cognitivo, para dar lugar a determinadas configuraciones híbridas complejas. Así, la adaptación militar se refiere a detectar el control de los equipos y a ser sinónimo de innovación doctrinal, transformación organizativa, pro-

tección de determinadas infraestructuras críticas, integración de capacidades, con el enriquecimiento del conocimiento estratégico en entornos de incertidumbre (Serrano Cuervo, 2026a; Serrano-Cuervo, 2026d).

Además, esta serie de nuevas transformaciones obligan a replantear la forma de entender la guerra. El pensamiento lineal, fragmentario, orientado por relaciones causales simples resulta muy difícil para la comprensión de conflictos donde las dimensiones físicas, digitales, cognitivas, sociales, informacionales y políticas interaccionan al mismo tiempo. El pensamiento complejo como un marco de referencia se presenta, en esta línea, particularmente útil para entender los sistemas militares contemporáneos como sistemas complejos adaptativos de carácter sociotécnico en los que los efectos de la acción militar no dependen en exclusiva de la suma de capacidades, sino de las relaciones, interdependencias o dinámicas emergentes entre actores, tecnologías, doctrinas, datos y contextos operacionales (Morin, 1990; Serrano-Cuervo 2026c).

En este sentido, el impacto de las nuevas tecnologías dentro de los escenarios de operaciones futuras no puede verbalizarse solamente como innovación material, sino también como transformación cognitiva, doctrinal e institucional. Dicho de otra forma, la pregunta en la que realmente se centra la cuestión estratégica no es solo la de introducir inteligencia artificial, drones, automatización, ciberdefensa o capacidades espaciales, sino determinar cómo tecnologías que han ido en aumento reconfiguran la capacidad de entendimiento del entorno, la toma de decisiones, la coordinación en el dominio y cómo encuentran esos efectos estratégicos en conflictos cada vez más densos en información, velocidad y ambigüedad (Scharre, 2018; Freedman, 2019; Serrano-Cuervo, 2026c; Serrano-Cuervo, 2026d).

Desde esta perspectiva, en este capítulo se intenta dar respuesta a la pregunta: ¿cómo deben evolucionar los sistemas de defensa multicapa para responder eficazmente a amenazas simultáneas en los dominios aéreo, terrestre, marítimo, espacial y ciber, en un entorno caracterizado por la convergencia tecnológica y la competencia multidominio?

Dado lo anterior, el presente capítulo formula como tesis central que la capacidad incisiva de las nuevas tecnologías en los escenarios de operaciones futuras no se ubica en plataformas sueltas y aisladas, sino por la capacidad de reconfigurar arquitecturas adaptativas de combate, defensa, *aware*, resiliencia,

decisión y multidominio. Es decir, el campo de juego estratégico del futuro no dependerá de la simple tenencia de tecnología, sino de las habilidades para intercalar sistemas de sistemas que sean capaces de aprender, retroceder, llevar a cabo coordinaciones y ejecutar acciones con sentido bajo presión. Por lo tanto, el objeto empírico de este capítulo son las arquitecturas de defensa aérea y antimisil integradas (*Integrated Air and Missile Defence* – IAMD) que se extienden a una defensa multicapa multidominio.

Por ello, desde una aproximación metodológica, la propuesta se presenta como un capítulo de divulgación de investigación científica basada en una revisión documental cualitativa y analítico-sintética de la literatura académica especializada, capítulos de libros de investigación, trabajos de estrategia, documentos doctrinales y última literatura sobre guerra tecnológica contemporánea, sistemas autónomos, defensa aérea, guerra híbrida, operaciones de los sistemas multiplataformas, resiliencia y adaptación militar. El análisis se soporta sobre los aportes de la teoría clásica y contemporánea de la guerra en el ámbito del análisis estratégico y sobre estudios recientes sobre el uso militar de las tecnologías emergentes y sus efectos sobre la seguridad y la defensa (Clausewitz, 2007; Freedman, 2019; Gray, 2015; Scharre, 2018; Serrano Cuervo, 2026a; Serrano-Cuervo, 2026b; Serrano-Cuervo, 2026c; Serrano-Cuervo, 2026d).

En otras palabras, no se plantea un estudio de caso completo ni una investigación empírica de campo; sino un ejercicio de síntesis interpretativa dirigido a traducir hallazgos científicos y desarrollos doctrinales en un marco de análisis útil para prever escenarios de operaciones. Para ello, se toman como referentes ilustrativos los conflictos y experiencias recientes (Ucrania, la confrontación Irán-Israel, la evolución de las amenazas híbridas en escenarios de alta complejidad) y discusiones relativamente aplicadas para el contexto colombiano y latinoamericano. El valor del capítulo se centra en la evolución de los sistemas de defensa aérea y antimisil integrados, como núcleo de la defensa multicapa frente a amenazas combinadas en los dominios aéreo, terrestre, marítimo, espacial y ciber.

Sistemas de defensa multicapa: bases conceptuales y evolución inicial

Los sistemas de defensa multicapa se definen como un tipo de arquitectura defensiva para dar respuesta a las amenazas aéreas y a las amenazas misilísticas que puede tener un Estado. Se desarrollan articulando múltiples sensores, interceptores, nodos de mando y control y capacidades de protección dispuestos en múltiples capas a diferentes distancias, a diferentes altitudes, en diferentes horizontes temporales, y teniendo en cuenta diferentes tipos de objetivo. Su lógica no reposa sobre la autosuficiencia de un único sistema, se enfatiza en el complemento de capas superpuestas que incrementan la probabilidad de detección, seguimiento, identificación y neutralización de múltiples amenazas que se articulan en situaciones de saturación, ambigüedad y presión temporal (Rozman, 2020; Stafford, 2021; Serrano Cuervo, 2026a).

Se puede considerar, desde un punto de vista conceptual, la defensa multicapa como un tipo de defensa en profundidad adaptada a los entornos aeroespaciales y misilísticos actuales. Es decir, mientras la defensa en profundidad es entendida como la asimilación, desgaste y desestructuración del enemigo a través de líneas sucesivas de resistencia; la defensa multicapa desplaza esa lógica en la que una situación de riesgo reúne a distintas partes para que una amenaza sea interceptada en distintos puntos de su trayecto, mediante distintos medios y desde distintas posiciones del sistema de defensa. De esta manera, la capacidad de defensa no depende de una oportunidad, sino de una secuencia escalonada de distintas oportunidades de intervención que atenaza el riesgo de penetración, distribuyendo la carga de la defensa entre partes distintas del sistema (Broch Hueso, 2012; Rozman, 2020).

La defensa aérea, en su primera versión, estaba orientada fundamentalmente a contrarrestar aeronaves tripuladas por medio de artillería antiaérea, radares e interceptores. No obstante, la incorporación progresiva de misiles balísticos, misiles de crucero, municiones guiadas, y, más recientemente, de drones y de enjambres, amplió tanto el espectro de amenazas que consideró insuficiente la distinción clásica entre defensa antiaérea y defensa antimisil. Por lo que el concepto de *Integrated Air and Missile Defense* (IAMD) haya cobrado especialmente sentido, ya que trata de integrar las dos funciones bajo el mismo entramado, doctrinalmente compatible y tecnológicamente interoperable (Rozman, 2020; Stafford, 2021; Muravska, 2023).

Por lo tanto, la asociación entre la defensa multicapa y la defensa aérea y antimisil es de carácter estructural. La defensa multicapa es la lógica arquitectónica y operativa mediante la cual la defensa aérea y antimisil puede reaccionar ante amenazas heterogéneas y simultáneas. No se trata únicamente de poseer capacidades de corto, medio o largo alcance, sino de integrar holísticamente las capacidades de corto, medio y largo alcance por medio de una red correspondiente que coadyuve a la vigilancia, la detección temprana, la adjudicación de objetivos, la autorización de fuego, la evaluación de daños y la asignación o reasignación de los recursos. Por consiguiente, una defensa multicapa de calidad no puede existir sin un buen y poderoso sistema de mando y control, sin enlaces de datos con una fiabilidad considerable y sin las doctrinas de empleo capaces de priorizar las amenazas y de coordinar las respuestas en momentos de alta compresión del tiempo operacional (Stafford, 2021; IAMD CoE, 2023; Serrano-Cuervo, 2026d).

La lógica multicapa responde a la variedad de vectores y perfiles de amenaza a los que se enfrentan las fuerzas. Una primera capa, normalmente de largo alcance, pretende detectar e interceptar la amenaza desde la mayor distancia posible, antes de que pueda cruzar ciertas líneas o zonas donde se concentran la población, infraestructuras críticas, zonas de despliegue de fuerzas y otras áreas de especial interés. Una segunda capa, de medio alcance o de área, se dirige a proteger zonas operacionales más concretas, o a enfrentarse a amenazas que han sobrepasado la capa externa de defensa. Por último, una tercera capa, de defensa de punto o terminal, se puede aplicar de manera más reducida a la protección de blancos especialmente sensibles mediante sistemas de muy corto alcance, armas de proximidad o soluciones de reacción inmediata. La justificación de esta estructura es de doble sentido: por una parte, la de tener redundancias; por la otra, la de asociar a toda amenaza el medio más idóneo de acuerdo con su velocidad, altitud, capacidad de maniobra, firma y probabilidad de daño (Broch Hueso, 2012; Rozman, 2020; Rehberg & Kemp, 2023).

Así, esta estructuración en capas tiene que ser entendida desde una concepción de integración. En el nivel técnico, integrar significa la conjunción de la información de radares, de sensores pasivos, de plataformas aéreas, navales y terrestres junto con su traducción a un cuadro operacional común. En el nivel funcional, exige coordinación entre los sensores, entre los tiradores y los mandos. En el nivel doctrinal, es impensable sin reglas sobre la prioridad de los

objetivos, sobre la asignación de los interceptores y sobre el empleo fusionado de las capacidades. Finalmente, a nivel estratégico, se considera la interoperabilidad entre servicios y, en algunos casos, entre socios ya que la defensa aérea y antimisil moderna frecuentemente se debe desbordar el de un solo servicio, o incluso de un solo país (IAMD CoE, 2023; Muravska, 2023; Stafford, 2021).

La dimensión integradora es relevante dado que las amenazas del siglo XXI no se presentan manera aislada. Tal como ha puesto de manifiesto la experiencia reciente, los ataques complejos, combinan drones, cohetes, misiles de crucero, vectores balísticos, guerra electrónica y, eventualmente, afectan la comunicación cibernética sobre sensores o redes de mando y control. En consecuencia, la defensa multicapa moderna no se puede concebir simplemente como una sucesión de baterías antiaéreas, sino como un sistema de sistemas, y la resiliencia de este depende de la coherencia funcional entre la detección, decisión, comunicación e interceptación. Esta lectura está en sintonía con esos marcos de referencia que han entendido las arquitecturas militares contemporáneas como sistemas complejos adaptativos, donde la ventaja se obtiene con la capacidad del material y con la capacidad de mezclar información, adaptarse a la fricción y mantener la funcionalidad bajo presión de multidominio (Serrano-Cuervo, 2026c; Serrano Cuervo, 2026a).

La evolución inicial que tomaron estos sistemas puede ser entendida como el camino que va de una defensa antiaérea orientada a plataformas a una defensa integrada centrada en capacidades. Así, en un primer momento, aparece una defensa puntual o sectorial, que va en primer lugar con la defensa dirigida a proteger bases, ciudades o formaciones de la aviación enemiga o adversaria. Después, la llegada de los misiles balísticos y de crucero, el desarrollo de redes de sensores y de enlaces de datos empujó a los formatos de defensa de teatro más extensos. Más recientemente, la aparición de amenazas simultáneas, distribuidas y de menor coste relativo (drones, municiones merodeadoras o ataques saturados) dieron a la defensa en sí, una cobertura, un sentido de integración en cuanto a la economía de la interceptación, la distribución de funciones y la resistencia operativa (Rozman, 2020; Stafford, 2021; Rehberg & Kemp, 2023).

Desde este contexto, los sistemas de defensa multicapa son parte de una respuesta evolutiva a la transformación del carácter de la guerra. Nuevas tecno-

logías no cambian la naturaleza política del conflicto, pero sí cambian profundamente los medios, ritmos y vulnerabilidades a través de los cuales ejercer coerción. Así, la defensa debe configurarse como defensa de una arquitectura estratégica que articule sensores, redes, plataformas, datos, infraestructura crítica y procesos de decisión. Esta evidencia será reveladora para los siguientes apartados del capítulo, cuando se procederá a describir cómo esta defensa multicapa debe transformarse para hacerle frente a las amenazas simultáneas en los dominios aéreo, terrestre, marítimo, espacioso y ciber (Serrano Cuervo, 2026a; Serrano-Cuervo, 2026d; Muravska, 2023).

Transformación del entorno estratégico y de las amenazas

La adaptación moderna del marco estratégico ha modificado la naturaleza operativa e histórica de las amenazas que se ciernen sobre los sistemas de defensa. En cuanto a la naturaleza política de la guerra no ha cambiado, sí que lo ha hecho su carácter, pero a causa de la fusión de tecnologías frontera, del ritmo de la toma de decisión, de la proliferación de actores no estatales, de la extensión del conflicto a nuevos escenarios y de la cada vez mayor combinación de medios cinéticos y no cinéticos (Freedman, 2019; Gray, 2015; Serrano Cuervo, 2026a). Por lo tanto, la amenaza actual ya no se puede entender como un vector único y lineal sino como una configuración compleja, diseminada y simultánea que busca saturar, desorganizar y degradar arquitecturas completas de defensa.

La primera transformación fue de la amenaza. En el marco del paradigma clásico, la defensa aérea y antimisil se organizaba en función de categorías más o menos bien diferenciadas: aeronaves tripuladas, misiles balísticos, misiles de crucero o ataques de artillería. En el contexto contemporáneo, esas categorías se entremezclan y combinan con drones de vigilancia y de ataque, municiones merodeadoras, enjambres, vectores de bajo coste, operaciones electrónicas, ciberataques y operaciones de información que darán lugar a amenazas híbridas que explotan, de manera simultánea, varias vulnerabilidades del sistema defensivo (IAMD CoE, 2023; Serrano-Cuervo, 2026d; Rogers & Kunertova, 2022). La amenaza, por tanto, ha dejado de ser un objeto netamente físico por interceptar y se ha convertido, también, en una dinámica de presión multisistémica conducida a poner en tensión la detección, la decisión y la respuesta.

La segunda transformación se encuentra interrelacionada con la convergencia de los dominios. Ya no se vive el conflicto contemporáneo únicamente en el dominio aéreo, pues se puede apreciar una interpolación continua de todo el dominio terrestre, de todo el dominio marítimo, del dominio espacial y del dominio ciberespacial. Los sistemas de defensa aérea y antimisil se sustentan en los sensores en tierra, los radares en el mar, los vínculos por satélites, la arquitectura digital relativa al mando y control, y unas redes de comunicaciones que son susceptibles de la interferencia, de la intrusión y de la degradación. Por esta razón, un ataque contundente contra un sistema de defensa aérea no implica necesariamente su destrucción, sino que puede ir, por ejemplo, contra la arquitectura de los datos, la cadena de logística, la conectividad, la construcción de un cuadro operacional común (Rozman, 2020; Stafford, 2021; Muravska, 2023). La amenaza multidominio ataca, por lo tanto, al sistema en su carácter de sistema funcional total.

La tercera transformación es la saturación como lógica de la ofensiva. Se podría sugerir que, en los conflictos más recientes, el problema fundamental de la defensa no es sólo lo letal de un vector, sino la capacidad que tiene un adversario de combinar formas de amenazas de bajo, medio y alto costo que tiendan a sobrepasar tiempos de reacción, a agotar interceptores, a forzar decisiones subóptimas y a quebrantar coberturas defensivas. Así pues, la saturación debe ser entendida en aspectos cuantitativos y cualitativos: un ataque puede saturar por volumen, por cantidad de vectores, por tiempo cronológico, por degradación electrónica o por la manipulación de prioridades en el sistema defensor (Jensen & Atalan, 2025; Boban, 2025; Rehberg & Kemp, 2023). Por lo tanto, debe tomarse en consideración que la saturación opera a partir de la arquitectura material de la defensa y también depende de la arquitectura cognitiva.

La experiencia ucraniana, y las escaramuzas entre Irán e Israel, indican el modelo anterior. Ambas partes ejecutaron contramedidas de forma compleja utilizando drones, misiles de crucero, cohetes, etc. De esta forma, provocan que el sistema defensivo redistribuyera capacidades, discriminara amenazas en poco tiempo y mantuviese la coherencia en fuego. En este sentido, la defensa se mide en supuestos valores de capacidad de derribo y se evalúa como resiliencia al agotamiento, como redundancia de sensores, como elasticidad maniobrando mando y control, como economía interceptora (Fox, 2021; Fox, 2026; Gürsu, 2026; Jensen & Atalan, 2025). Así, la saturación se entendería como un

pase de la defensa por un contrapunto de competición gradual entre el coste ofensivo y la sostenibilidad defensiva.

Por tanto, la lógica se ve complementada por la velocidad como elemento estructural del entorno estratégico, el aumento progresivo de la velocidad de los vectores, la reducción de los tiempos de parada y de decisión, o la automatización creciente de los ciclos de combate, se han ocupado de reducir el espacio temporal del que gozan la deliberación humana. Esta compresión se extiende a las amenazas hipersónicas o balísticas y a golpes combinados donde la velocidad decisional que tenga el sistema será tan relevante como la rapidez física del vector. Por lo que la superioridad radica en tener mejores interceptores y en ser mejores en recorrer los ciclos de observación, orientación, decisión y acción en situaciones de alta fricción (Boyd, 2018; Stafford, 2021; Serrano-Cuervo, 2026d). La velocidad redefine así la relación que existe entre la tecnología, el mando y el juicio estratégico.

La automatización es una quinta transformación importante. La introducción de la inteligencia artificial, el aprendizaje automático, la automatización mediante sensores, los algoritmos de clasificación y sistemas de apoyo a la decisión modifican la forma de detectar, clasificar y gestionar las amenazas. Estas herramientas tienen ventajas en contextos de saturación y limitación de tiempo. Son útiles para procesar grandes volúmenes de información, para identificar patrones en los datos y para facilitar la asignación de los recursos de defensa. Pero al tiempo que traen ventajas, también son fuentes de nuevas vulnerabilidades: a) dependen de arquitecturas digitales muy específicas, b) son vulnerables a ataques informáticos, c) no ofrecen transparencia algorítmica, y d) son susceptibles de errores en una velocidad en la que la rapidez operacional está muy presente (Scharre, 2018; Serrano-Cuervo, 2026d; Russell, 2019). La automatización no elimina la necesidad de que los humanos se pronuncien sobre los problemas, sino que los desplaza a la calidad de la integración entre humanos y máquinas en el sistema de defensa.

Otra característica que define el entorno contemporáneo es la creciente prominencia de los actores no estatales que implementan capacidades tecnológicas de vanguardia. Drones comerciales modificados, munición guiada, sistemas de navegación, plataformas de observación, armas de ataque remoto y un ingenio enorme que antiguamente se reservaban para el Estado o las grandes fuerzas

armadas, han sido capaces de ser implementados por grupos armados no estatales, milicias, proxies u organizaciones híbridas. Entonces, en función de la oferta tecnológica, se ha despojado de las restricciones de acceso e introducido a los actores no estatales como actores capaces de mezclar tácticas irregulares o asimétricas con movimientos de exactitud, saturación y alcance (Chávez & Swed, 2020a; Chávez & Swed, 2020b; Jokinen & Normark, 2022). Esto da como resultado una amenaza menos predecible, menos centralizada y más difícil de acotar y neutralizar en muchos casos.

La relación entre actores estatales y no estatales complica aún más el cuadro. En contextos diversos, la amenaza no reside en una separación clara o una separación tajante entre guerra interestatal y violencia irregular, sino que también, en algunas configuraciones híbridas, que son muy habituales. Hay Estados que apoyan proxies, transfieren tecnología, externalizan presión o eligen un entorno de ambigüedad del que extraer las herramientas necesarias para mantener la confrontación por debajo de los umbrales político-jurídicos exigidos. Resulta que la defensa debe prepararse para grandes campañas convencionales y para campañas de desgaste, de acoso, o de prueba de sistemas mediante acciones limitadas, distribuidas y reiterativas (Hoffman, 2007; Rauta, 2019; Serrano Cuervo, 2026a).

Atacar ya no siempre significa la destrucción inmediata; se trata de la erosión gradual de la capacidad de decisión y de la voluntad de resistencia. A nivel estratégico, estas transformaciones abren nuevas líneas de pensamiento para abordar la concepción de la defensa multicapa. La amenaza actual es simultánea, híbrida, distribuida, ágil, automatizada y potencialmente escalable por parte de agentes estatales y no estatales. Por tanto, una respuesta defensiva no podría limitarse a la multiplicación de sistemas de armas, sino que debería ser capaz de construir arquitecturas de modo que integren los dominios; soporten la saturación; sostengan la resiliencia o mantengan la coherencia operativa en situaciones en las que los ataques sean, por ejemplo, combinados. Así, la transformación del entorno estratégico no es un telón de fondo, sino la condición para limitar el porqué de la defensa multicapa entendida como una lógica fundamentalmente área a una lógica verdaderamente multidominio (Rozman, 2020; Rehberg & Kemp, 2023; Muravska, 2023).

Por tanto, el entorno estratégico actual ha dejado atrás la imagen de la amenaza única y secuencial. Surge entonces un ecosistema de confrontación en donde emergen vectores distintos, dominios interdependientes, presión temporal, automatización creciente y pluralidad de actores con capacidad de generar efectos estratégicos. Esta transformación es clave para entender cómo evolucionarán los sistemas de defensa multicapa si ambicionan evitar con eficacia las amenazas de manera simultánea en los dominios aéreo, terrestre, marítimo, espacial y ciber. Ese será, en efecto, el punto de inicio del segmento siguiente del capítulo.

Limites del modelo clásico de defensa antiaérea

El modelo clásico de defensa antiaérea fue concebido para enfrentar amenazas relativamente diferenciadas, secuenciales y previsibles, en un entorno donde predominaban aeronaves tripuladas, corredores de aproximación más definidos y ciclos de decisión menos comprimidos. En ese contexto, la defensa se organizaba con frecuencia alrededor de la protección de áreas limitadas, bajo estructuras de mando centralizadas, sectores rígidamente delimitados y una separación funcional entre sensores, centros de decisión y armas. Sin embargo, la transformación del entorno estratégico y de las amenazas ha puesto en evidencia limitaciones crecientes de ese modelo, particularmente frente a ataques simultáneos, distribuidos y multidominio (Rozman, 2020; Stafford, 2021; Serrano Cuervo, 2026a).

Un primer límite es la rigidez doctrinal. La doctrina clásica de defensa antiaérea fue diseñada para proteger objetivos fijos o concentraciones de fuerza frente a incursiones aéreas relativamente identificables, privilegiando geometrías estáticas de cobertura, secuencias formales de autorización de fuego y una fuerte dependencia de jerarquías superiores para la coordinación del combate. Este enfoque resulta crecientemente insuficiente cuando la amenaza ya no se presenta en forma lineal, sino como combinación de drones, misiles de crucero, vectores balísticos, saturación electrónica y ciberafectación de redes. En ese entorno, doctrinas basadas en áreas limitadas, cobertura sectorial fija y supuestos de previsibilidad reducen la capacidad de adaptación del sistema defensivo y generan respuestas más lentas que el ritmo del ataque (Rozman, 2020; Molina, 2025; IAMD CoE, 2023).

Esta rigidez doctrinal se agrava por la persistencia de una visión todavía demasiado centrada en plataformas y no en arquitecturas de defensa. En el modelo clásico, la eficacia se asociaba con la posesión de baterías, cañones, radares o interceptores específicos, mientras que en el entorno contemporáneo la eficacia depende crecientemente de la integración funcional entre esos elementos. Cuando la doctrina permanece anclada en la defensa puntual o en la lógica de “sistema por sistema”, se dificulta la transición hacia esquemas de defensa multicapa, distribuidos y adaptativos. Como advierte Stafford (2021), la evolución hacia operaciones multidominio exige pasar de una defensa basada en sectores y plataformas a otra basada en redes, fusión de sensores y autoridad de respuesta más flexible. La permanencia de marcos doctrinales heredados se convierte, por tanto, en un freno para la adaptación institucional.

Un segundo límite estructural es la fragmentación de sensores. En las arquitecturas clásicas, los radares y demás medios de detección solían operar en cadenas relativamente jerarquizadas y con escasa interoperabilidad lateral, lo que producía imágenes parciales del entorno aéreo y reducía la capacidad de seguimiento continuo de amenazas complejas. Esta fragmentación era manejable en escenarios menos densos y con un número más limitado de vectores. Sin embargo, en el contexto actual, donde conviven amenazas múltiples, trayectorias variables, vuelos rasantes y ataques desde distintos dominios, la ausencia de fusión integral de sensores genera puntos ciegos, duplicación de esfuerzos y dificultades de priorización (IAMD CoE, 2023; Großwald Systems Desk, 2026). En consecuencia, la defensa ya no puede descansar en una secuencia lineal de “sensor-central-arma”, sino en una red de sensores interoperables capaz de producir un cuadro operacional común en tiempo casi real.

La fragmentación de sensores no es solo un problema técnico, sino también organizacional y cognitivo. Cuando cada unidad o capa opera con su propia imagen táctica, la coordinación se vuelve más lenta y vulnerable al error. La falta de integración incrementa el riesgo de fratricidio, de asignaciones redundantes de interceptores o de pérdida de ventanas de *engagement* por demoras en la decisión. Los entornos multidominio exacerban ese problema porque exigen combinar información procedente de plataformas aéreas, terrestres, navales, espaciales y, cada vez más, cibernéticas. El modelo clásico, al no haber sido diseñado para esta densidad y simultaneidad de datos, muestra una capacidad

limitada para transformar información dispersa en decisión operativa coherente (Hawley *et al.*, 2005; Priebe *et al.*, 2020; Serrano-Cuervo, 2026d).

Un tercer límite decisivo es la dependencia de jerarquías lentas. En la defensa antiaérea clásica, la centralización del mando respondía a la necesidad de mantener control del espacio aéreo, evitar fuegos indiscriminados y coordinar escasos recursos de alto valor. No obstante, esa arquitectura introduce latencias incompatibles con amenazas actuales que comprimen el tiempo entre detección, clasificación, decisión y disparo. Cuando la autoridad está excesivamente concentrada en niveles superiores, las capas tácticas pierden capacidad de reacción y el sistema corre el riesgo de llegar tarde, incluso si dispone de sensores y armas adecuadas. La literatura sobre IAMD muestra con claridad que la coexistencia de amenazas veloces, múltiples y simultáneas obliga a reconsiderar la distribución de autoridad y la autonomía táctica dentro de marcos doctrinales seguros (Corey, 2017; Stafford, 2021; Großwald Systems Desk, 2026).

La lentitud jerárquica se vuelve todavía más crítica en ataques distribuidos. Un sistema centralizado puede gestionar razonablemente un número limitado de aproximaciones, pero encuentra dificultades crecientes cuando debe coordinar respuestas en múltiples puntos del teatro, proteger nodos dispersos o decidir bajo degradación parcial de comunicaciones. Priebe *et al.*, (2020), han señalado, en el contexto del *all-domain command and control*, que las operaciones que dependen de aprobaciones externas, largos circuitos de coordinación o comunicaciones estables resultan especialmente vulnerables en ambientes contestados. Aplicado a la defensa antiaérea, esto significa que el modelo clásico tiende a producir una paradoja: cuanto más busca controlar todo desde arriba, más expuesto queda a perder efectividad cuando la complejidad del combate exige agilidad en los bordes del sistema.

El cuarto límite central es la dificultad para enfrentar ataques simultáneos y distribuidos. La defensa antiaérea clásica fue pensada para repeler incursiones relativamente concentradas sobre objetivos clave. En contraste, los ataques actuales pueden combinar oleadas de drones, misiles de crucero, cohetes, *decoys*, interferencia electrónica y acciones sobre redes de mando y control, distribuidas en tiempo y espacio para obligar al defensor a dispersar su atención y sus recursos. En este contexto, el problema ya no es solo si un sistema puede derribar un blanco, sino si una arquitectura completa puede sostenerse funcio-

nalmente frente a múltiples presiones simultáneas. Los modelos clásicos, centrados en defensa puntual, geometrías fijas y secuencias jerárquicas, muestran serias dificultades para escalar hacia este tipo de combate (Rehberg & Kemp, 2023; Jensen & Atalan, 2025; Molina, 2025).

Además, el modelo clásico enfrenta limitaciones frente a la economía de desgaste que caracteriza muchas campañas contemporáneas. La proliferación de drones baratos, municiones merodeadoras y vectores de bajo costo erosiona la lógica tradicional de usar interceptores caros contra amenazas individualmente significativas. Cuando la defensa carece de flexibilidad doctrinal, integración sensorial y capacidad de asignar distintos medios según la naturaleza del ataque, se expone a una asimetría desfavorable entre costo ofensivo y costo defensivo. Así, un sistema concebido para repeler amenazas de alto valor unitario puede verse desbordado por campañas de saturación prolongada que explotan su rigidez y lo fuerzan a consumir recursos estratégicos en escenarios tácticamente degradantes (Jensen & Atalan, 2025; Boban, 2025).

En conjunto, estos límites muestran que el problema del modelo clásico de defensa antiaérea no radica en que sus principios hayan perdido toda validez, sino en que fueron concebidos para un entorno menos interdependiente, menos veloz y distribuido. La doctrina jerárquica, la organización sectorial, la separación de sensores y la lógica de defensa puntual siguen teniendo utilidad en ciertos contextos, pero resultan insuficientes como base exclusiva para responder al carácter contemporáneo de la amenaza. Desde esta perspectiva, la evolución hacia sistemas de defensa multicapa y multidominio no representa una ruptura arbitraria, sino la adaptación necesaria frente a un entorno en el que la defensa ya no puede limitarse a cubrir el cielo, sino que debe proteger una arquitectura compleja de sensores, redes, decisiones y nodos distribuidos (Rozman, 2020; Serrano Cuervo, 2026a; Serrano-Cuervo, 2026d).

Comprender estos límites es fundamental porque permite identificar con mayor precisión qué debe cambiar. El problema no es únicamente tecnológico, sino también doctrinal, organizacional y cognitivo. De ahí que el siguiente paso del análisis consista en examinar cómo deben evolucionar los sistemas de defensa multicapa para superar estas restricciones, ganar adaptabilidad y responder eficazmente a amenazas simultáneas en los dominios aéreo, terrestre, marítimo, espacial y ciber.

De la defensa antiaérea a la defensa multidominio

La evolución desde la defensa antiaérea clásica hacia una defensa multidominio constituye una respuesta adaptativa a la transformación del entorno estratégico y a los límites estructurales del modelo heredado. Este tránsito implica reconfiguración de la defensa antiaérea dentro de una arquitectura más amplia que integra defensa aérea, antimisil, ciberresiliencia, apoyo espacial, fusión de sensores y coordinación interdominio. En otras palabras, el cambio consiste en añadir nuevas tecnologías a una estructura preexistente y en producir un salto doctrinal, operacional y tecnológico que permita responder a amenazas simultáneas y distribuidas en los dominios aéreo, terrestre, marítimo, espacial y ciber (Rozman, 2020; Stafford, 2021; IAMD CoE, 2023).

El primer componente de este tránsito es doctrinal. La defensa antiaérea clásica descansaba en doctrinas centradas en la protección del espacio aéreo inmediato, la sectorización rígida, la defensa puntual y la secuencia lineal detección-decisión-intercepción. La lógica multidominio, por el contrario, exige comprender la defensa como una función transversal de la campaña, orientada a preservar la libertad de acción propia y a negar al adversario la capacidad de producir efectos sistémicos. Desde esta perspectiva, la defensa no se limita al derribo de vectores, sino que busca proteger la arquitectura funcional del sistema: sensores, redes, mando y control, logística, datos, infraestructura crítica y enlaces con otros dominios (Reilly, 2016; Rozman, 2020; Gady & Stronell, 2020). El salto doctrinal consiste, entonces, en pasar de una defensa del "espacio aéreo" a una defensa de la "coherencia operativa" del sistema conjunto.

Esta transformación doctrinal supone, además, una integración más estrecha entre defensa y maniobra. En el enfoque clásico, la defensa antiaérea operaba a menudo como función de protección relativamente separada del esfuerzo principal. En cambio, en la lógica multidominio, la defensa debe articularse con la maniobra terrestre, la protección marítima, la guerra electrónica, la ciberdefensa, la inteligencia y el uso del espacio como parte de una arquitectura convergente. La defensa deja de ser reactiva y se integra en esquemas más amplios de disuasión, supervivencia, continuidad operativa y explotación de ventajas temporales sobre el adversario. De ahí que varios desarrollos doctrinales recientes insistan en que la IAMD ya debe pensarse como componente

activo de las operaciones multidominio (Stafford, 2021; U.S. Air Force, 2025; Singh, 2024).

El segundo componente del tránsito es el operacional. La defensa multidominio requiere superar la lógica de sectores fijos y avanzar hacia arquitecturas distribuidas, móviles y resilientes. En el modelo clásico, los sensores y tiradores tendían a organizarse en cadenas relativamente jerarquizadas, con centros de control que concentraban gran parte de la información y la autoridad. En entornos de alta velocidad y ataques simultáneos, esa organización resulta vulnerable a saturación, degradación de comunicaciones y pérdida de nodos críticos. La evolución operacional exige, por ello, redes de sensores interoperables, cuadros operacionales compartidos, delegación controlada de autoridad y capacidad de combate incluso en condiciones degradadas o desconectadas (Pribe *et al.*, 2020; IAMD CoE, 2023; Rozman, 2020).

Este cambio operacional también implica pasar de una defensa puntual a una defensa escalonada y adaptativa. En una arquitectura multidominio, las capas no se entienden solo por alcance o altitud, sino también por función dentro del sistema: alerta temprana, identificación, interrupción, interceptación, defensa de punto, redundancia de redes y continuidad del mando. Además, la respuesta defensiva debe poder sincronizar medios terrestres, navales, aéreos y espaciales, e incorporar la dimensión ciber como condición de posibilidad de toda la arquitectura. La defensa de un nodo crítico no depende de su batería antiaérea, sino de la red que le proporciona conciencia situacional, comunicaciones, datos de *targeting* y protección frente a interferencia o intrusión. En este sentido, el salto operacional radica en una red defensiva conjunta y distribuida (Muravska, 2023; Dumitrescu, 2023; Großwald Systems Desk, 2026).

El tercer componente es el tecnológico. La transición a la defensa multidominio exige una evolución desde sistemas relativamente autónomos hacia arquitecturas integradas con procesamiento de información en tiempo real. Tecnológicamente, esto implica integrar radares de distintas bandas, sensores pasivos, plataformas aéreas y navales, capacidades espaciales, inteligencia artificial aplicada a clasificación y priorización de amenazas, y redes de mando y control capaces de operar bajo degradación parcial. Se trata de construir una malla tecnológica que convierta datos dispersos en decisión operativa coherente (Scharre, 2018; Russell, 2019; Serrano-Cuervo, 2026d).

Ahora bien, este salto tecnológico no puede interpretarse como solución puramente instrumental. La experiencia contemporánea muestra que incorporar IA, automatización o nuevos sensores sobre doctrinas rígidas y cadenas lentas no resuelve el problema de fondo. Si la arquitectura sigue organizada para un entorno lineal y secuencial, la tecnología solo acelera una lógica ya insuficiente. Por ello, la innovación tecnológica debe ir acompañada de transformación doctrinal y adaptación organizacional. El verdadero salto es convertirla en una arquitectura multidominio donde sensores, nodos, operadores y mandos funcionen como parte de un sistema complejo adaptativo (Serrano-Cuervo, 2026c; Serrano-Cuervo, 2026d).

Desde esta perspectiva, el paso de la defensa antiaérea a la defensa multidominio puede entenderse como una transición desde la lógica del "escudo" hacia la lógica de la "red". El escudo remite a una imagen estática, sectorial y predominantemente reactiva; la red, en cambio, supone interdependencia, distribución, aprendizaje y adaptabilidad. En una defensa multidominio, el objetivo es interceptar lo que viene del aire y proteger la capacidad del sistema para detectar, decidir, coordinar y actuar a través de varios dominios simultáneamente. Esta transición explica por qué la interoperabilidad, la conectividad, la resiliencia y la capacidad de operar con información incompleta se han vuelto tan decisivas como el rendimiento cinético de los interceptores (Stafford, 2021; Priebe *et al.*, 2020; IAMD CoE, 2023).

El carácter propositivo de esta evolución también exige reconsiderar la relación entre centralización y descentralización. La defensa multidominio no elimina la necesidad de mando central, pero sí obliga a combinar dirección estratégica con mayor autonomía táctica y capacidad de adaptación local. En la medida en que los ataques sean simultáneos, distribuidos y multidominio, la defensa eficaz dependerá de arquitecturas de mando capaces de conservar coherencia sin depender de un único nodo de decisión. Esto requiere nuevas doctrinas de misión, entrenamiento orientado a la adaptación, reglas de empuñamiento más flexibles y una cultura institucional menos dependiente de secuencias jerárquicas rígidas (Reilly, 2016; Priebe *et al.*, 2020; Stafford, 2021).

En suma, la transición de la defensa antiaérea a la defensa multidominio representa un salto cualitativo en tres planos convergentes. Doctrinalmente, implica pasar de la protección del espacio aéreo a la protección de la arquitectura

operativa conjunta. Operacionalmente, exige transformar cadenas sectoriales en redes distribuidas y resilientes. Tecnológicamente, supone integrar sensores, datos, automatización y ciberresiliencia dentro de un sistema capaz de sostener coherencia bajo presión multidominio. Este salto es la condición necesaria para superar los límites del modelo clásico y sentar las bases de una defensa multicapa apta para el entorno contemporáneo.

Componentes de la evolución del sistema multicapa

La evolución de un sistema de defensa multicapa hacia una arquitectura verdaderamente multidominio no depende únicamente de aumentar el número de interceptores o ampliar el rango de cobertura. Su eficacia futura descansará, sobre todo, en la capacidad para articular componentes técnicos, organizacionales y doctrinales en una arquitectura abierta, interoperable, modular y resiliente. Esto implica superar soluciones cerradas, integraciones verticales rígidas y cadenas secuenciales de sensores, mando y fuego, para avanzar hacia un sistema de sistemas capaz de adaptarse a amenazas simultáneas, saturadas y distribuidas (Rozman, 2020; Stafford, 2021; Serrano-Cuervo, 2026d).

Un primer componente esencial es la arquitectura abierta. Los modelos cerrados o propietarios tienden a generar dependencias tecnológicas, dificultan la actualización de capacidades y limitan la incorporación de nuevos sensores o efectores en tiempo útil. Por el contrario, una arquitectura abierta se basa en estándares comunes, interfaces compartidas y diseño orientado a integración, lo que permite incorporar nuevos nodos sin rediseñar todo el sistema. En el ámbito de defensa, este enfoque se ha desarrollado bajo marcos como el *Modular Open Systems Approach* (MOSA), cuyo propósito es reducir el efecto de los “stovepipes” y facilitar soluciones *plug-and-play* más ágiles, sostenibles e interoperables (Department of Defense, 2020; Maurer *et al.*, 2006; Moulton *et al.*, 2015). Para un sistema multicapa, ello significa que radares, sensores pasivos, enlaces de datos, plataformas navales, unidades terrestres y aplicaciones de procesamiento deben poder integrarse sin quedar atados a una sola plataforma, un solo proveedor o una sola lógica de actualización.

La interoperabilidad constituye el segundo componente crítico. No basta con que los sistemas sean técnicamente compatibles; deben compartir datos, doc-

trinas, protocolos de identificación y procedimientos de empleo que permitan actuar como una red coherente. En términos operacionales, la interoperabilidad es la condición que convierte una suma de subsistemas en una arquitectura defensiva funcional. Esto incluye interoperabilidad entre fuerzas, entre servicios, entre dominios y, en ciertos contextos, entre aliados. La literatura reciente sobre IAMD muestra que la defensa aérea y antimisil contemporánea depende crecientemente de la capacidad para conectar sensores terrestres, plataformas aéreas, unidades navales, recursos espaciales y sistemas de mando y control bajo un cuadro operacional común y con reglas de empuñamiento coordinadas (IAMD CoE, 2023; Muravska, 2023; Rozman, 2020). Sin interoperabilidad, la defensa multicapa degenera en una agregación de islas tecnológicas con baja capacidad de respuesta conjunta.

El tercer componente es la fusión de sensores, que constituye el núcleo cognitivo de cualquier sistema de defensa multicapa evolucionado. En el entorno estratégico actual, ninguna fuente sensorial aislada puede proporcionar por sí sola una imagen suficiente del campo de amenazas. Las firmas bajas, los vuelos rasantes, la velocidad de ciertos vectores, la saturación y la acción simultánea en varios dominios exigen combinar información procedente de radares de distintas bandas, sensores pasivos, plataformas aéreas, satélites, sistemas navales, inteligencia electrónica y otras fuentes. La fusión sensorial mejora la detección e incrementa la capacidad de seguimiento, clasificación y asignación de recursos defensivos bajo presión temporal (Maurer *et al.*, 2006; Frenkel, 1994; Dahlgren *et al.*, 2025). En este sentido, el futuro del sistema multicapa depende de la calidad de sus sensores y de su capacidad para convertir múltiples flujos de datos en conocimiento operacional útil.

A ello se suma la necesidad de una malla sensorial distribuida, o *mesh sensing*, como evolución de la arquitectura tradicional basada en pocos sensores de alto valor. Los sistemas más avanzados tienden a combinar sensores activos y pasivos, nodos fijos y móviles, plataformas tripuladas y no tripuladas, así como cobertura terrestre y espacial. Esta proliferación de sensores mejora la redundancia, reduce la vulnerabilidad frente a ataques a nodos críticos y permite sostener niveles aceptables de conciencia situacional incluso bajo degradación parcial. Para la defensa multicapa, ello es particularmente importante porque las amenazas actuales atacan con vectores físicos y, también, mediante opera-

ciones orientadas a cegar, engañar o sobrecargar la percepción del sistema (Dahlgren *et al.*, 2025; IAMD CoE, 2023).

El cuarto componente es la inteligencia artificial. En un entorno saturado de datos, con múltiples trayectorias simultáneas y ventanas de decisión muy reducidas, la IA se convierte en una herramienta relevante para filtrar información, detectar patrones, clasificar amenazas, priorizar objetivos y apoyar la asignación de interceptores. Su utilidad reside en reducir la carga cognitiva del operador y acelerar los ciclos de observación, orientación, decisión y acción. Sin embargo, la incorporación de IA debe entenderse como apoyo a la decisión y no como sustitución automática del juicio humano. La literatura advierte que la IA introduce vulnerabilidades relacionadas con sesgos de datos, opacidad algorítmica, errores de clasificación y susceptibilidad a manipulación adversarial, especialmente en contextos de guerra electrónica y ciberataques (Scharre, 2018; Russell, 2019; Topor, 2025). Por ello, la evolución del sistema multicapa exige una integración humano-máquina cuidadosamente diseñada, con validación cruzada, supervisión significativa y capacidad de degradar con elegancia en caso de fallo.

El quinto componente es la ciberresiliencia. En un sistema de defensa multidominio, la red es tan importante como el interceptor. Sensores, enlaces de datos, cuadros de situación, redes de mando y control, logística digitalizada y procesos de decisión automatizados amplían la capacidad del sistema, pero también abren superficies de vulnerabilidad. La ciberresiliencia implica diseñar el sistema para resistir, absorber, recuperarse y adaptarse frente a intrusiones, interferencias, corrupción de datos o pérdida de conectividad. Se trata de proteger servidores o redes y de asegurar continuidad funcional bajo condiciones degradadas. Un sistema multicapa verdaderamente evolucionado debe poder seguir operando, aunque sea con rendimiento reducido, aun cuando parte de su arquitectura digital haya sido afectada (Gady & Stronell, 2020; Serrano-Cuervo, 2026d; Priebe *et al.*, 2020). En este punto, la ciberdefensa deja de ser complemento y pasa a ser condición estructural de la defensa aérea y antimisil contemporánea.

Un sexto componente es el enlace entre dominios. La defensa multicapa del futuro no puede pensarse como asunto exclusivamente aéreo. Las trayectorias de ataque, la dependencia de infraestructura satelital, el uso de plataformas

navales como nodos de detección o interceptación, la afectación ciber de redes y el empleo de unidades terrestres móviles como efectores, muestran que el sistema defensivo solo será eficaz si conecta funcionalmente los dominios aéreo, terrestre, marítimo, espacial y ciber. Esto exige compatibilidad técnica y una doctrina capaz de entender cada dominio como fuente potencial de protección, soporte o degradación del sistema. La verdadera multidimensionalidad de la defensa multicapa radica precisamente en esta capacidad para operar como red interdominio, donde la afectación de un componente repercute sobre todos los demás y donde la ventaja proviene de la convergencia, no de la yuxtaposición (U.S. Air Force, 2025; Muravska, 2023; Rozman, 2020).

Finalmente, un séptimo componente es la adaptación modular. El modularidad permite que el sistema evolucione sin requerir reconstrucciones completas ante cada cambio tecnológico o amenaza emergente. Un sistema modular puede incorporar nuevos sensores, software, efectores, protocolos o capacidades de análisis sin comprometer la arquitectura general. Esto mejora la capacidad de actualización, reduce obsolescencia, facilita experimentación y permite respuestas más ágiles frente a la proliferación de vectores como drones, misiles hipersónicos o herramientas de disrupción digital (Department of Defense, 2020; U.S. Navy & U.S. Marine Corp., 2025; Vogler *et al.*, 2026). Para Estados con restricciones presupuestales o necesidades de adaptación progresiva, esta modularidad resulta especialmente relevante, pues permite evolucionar por capas funcionales y no solo por reemplazo total de sistemas.

En conjunto, estos componentes muestran que la evolución del sistema multicapa debe concebirse como un proceso de transformación integral. Arquitectura abierta, interoperabilidad, fusión de sensores, inteligencia artificial, ciberresiliencia, enlace entre dominios y adaptación modular no son atributos aislados, sino dimensiones interdependientes de una misma lógica de modernización. La ausencia de cualquiera de ellas introduce vulnerabilidades significativas: sin arquitectura abierta se dificulta la actualización; sin interoperabilidad no hay red funcional; sin fusión sensorial no hay conciencia situacional suficiente; sin IA el sistema puede quedar cognitivamente sobrecargado; sin ciberresiliencia se vuelve frágil; sin enlace entre dominios permanece encerrado en una visión parcial; y sin modularidad pierde capacidad de adaptación. La defensa multicapa del futuro, por tanto, deberá evolucionar menos como una suma de sistemas y más como arquitectura compleja, conectada y adaptable, orientada a soste-

ner coherencia operativa en escenarios de alta velocidad, saturación y convergencia multidominio (Serrano-Cuervo, 2026c; Serrano-Cuervo, 2026d; Stafford, 2021).

Implicaciones estratégicas, operacionales y doctrinales

La evolución de los sistemas de defensa multicapa hacia arquitecturas multidominio no es un asunto exclusivamente técnico. Sus implicaciones alcanzan la estrategia del Estado, la organización de las fuerzas armadas, la formulación doctrinal, el entrenamiento, la protección de infraestructura crítica y los procesos de toma de decisiones. En este sentido, la defensa multicapa debe entenderse como un componente estructural de la seguridad nacional contemporánea, especialmente en entornos donde convergen amenazas aéreas, misilísticas, cibernéticas, espaciales e híbridas (Pietrus, 2023; NATO, 2025; Serrano Cuervo, 2026a).

Desde una perspectiva estratégica, la principal implicación para los Estados es que la defensa debe concebirse contemporáneamente como una dimensión central de la disuasión, la resiliencia nacional y la libertad de acción estratégica. Un sistema multicapa eficaz incrementa el costo de la coerción adversaria, reduce la vulnerabilidad frente a ataques de precisión y fortalece la credibilidad política del Estado al proteger población, infraestructura crítica, nodos militares y continuidad gubernamental. Por ello, la IAMD ha pasado a ser considerada en varios entornos estratégicos como uno de los pilares de la seguridad nacional y de la disuasión defensiva por su efecto estabilizador sobre la postura estratégica general (Pietrus, 2023; NATO, 2025; van Hooft & Boswinkel, 2021). Esto implica que la inversión en defensa multicapa debe articularse con la estrategia nacional, y no permanecer confinada a una lógica puramente sectorial o de adquisición de sistemas.

Esta noción estratégica adquiere especial relevancia para Estados medianos o con limitaciones presupuestales. En estos casos, la pregunta central es cómo construir combinaciones realistas de protección, redundancia y priorización. La defensa multicapa obliga, por tanto, a definir qué activos constituyen verdaderos centros de gravedad nacionales, cuáles infraestructuras requieren protección prioritaria y qué equilibrio es viable entre cobertura nacional, defensa de

puntos críticos y movilidad de capacidades. En otras palabras, el salto estratégico exige pasar de una lógica de acumulación de medios a una lógica de selección estratégica de prioridades, donde la defensa se diseñe en función de vulnerabilidades críticas y no solo de aspiraciones maximalistas (Muravska, 2023; van Hooft & Boswinkel, 2021; Serrano-Cuervo, 2026d).

En el plano operacional, la principal consecuencia es la necesidad de reorganizar la relación entre sensores, tiradores, mandos y apoyos interdominio. Un sistema multicapa multidominio exige operaciones distribuidas, redes de datos resilientes, cuadros operacionales compartidos y capacidad de seguir combatiendo bajo degradación parcial. Esto obliga a superar estructuras excesivamente centralizadas y a construir mandos capaces de mantener coherencia sin depender permanentemente de comunicaciones perfectas o de un único centro decisional. La operación defensiva debe coordinar efectos sobre un teatro dinámico donde convergen ataques físicos, interferencias electrónicas, afectaciones ciber y presión sobre nodos logísticos (Rozman, 2020; Priebe *et al.*, 2020; Almodovar *et al.*, 2018). La consecuencia práctica es clara: la defensa multicapa del futuro requerirá una arquitectura operacional más distribuida, más flexible y mejor integrada con el resto de la maniobra conjunta.

Esto también transforma la relación entre defensa y sostenimiento. En escenarios de alta saturación, la eficacia no depende solo de la capacidad de interceptar, sino de sostener el sistema a lo largo del tiempo. De ahí que la logística, la reposición de interceptores, la protección de sensores, la supervivencia de nodos de mando y la continuidad energética y digital pasen a ser variables operacionales decisivas. Un sistema incapaz de regenerarse, redistribuirse o seguir funcionando tras pérdidas parciales puede colapsar aun si sus componentes individuales son técnicamente avanzados. Por ello, la defensa multicapa exige una concepción operacional más cercana a la resiliencia sistémica que a la simple capacidad de fuego (Stafford, 2021; van Hooft & Boswinkel, 2021; Davis, 2017).

En el plano doctrinal, la implicación más importante es la necesidad de revisar categorías heredadas que separan de forma rígida defensa aérea, defensa antimisil, ciberdefensa, guerra electrónica, protección de infraestructura y apoyo espacial. La doctrina deberá evolucionar hacia marcos que reconozcan explícitamente la convergencia de dominios y la interdependencia entre funciones.

Esto no significa eliminar especialidades, sino articularlas bajo una doctrina común de defensa multidominio que oriente el empleo de sensores, armas, nodos de decisión y apoyos desde una misma lógica operativa (IAMD CoE, 2023; U.S. Air Force, 2025; Serrano-Cuervo, 2026c). La defensa deja de ser una función aislada de ciertas armas o especialidades y pasa a ser una responsabilidad transversal del sistema conjunto.

Esta transformación doctrinal tiene efectos directos sobre el entrenamiento. Las fuerzas armadas deben incorporar ejercicios que simulen saturación, degradación ciber, pérdida de sensores, interferencia electrónica, presión temporal y operación conjunta con múltiples dominios. Asimismo, el entrenamiento debe fortalecer el juicio bajo incertidumbre, la comprensión del sistema como totalidad y la capacidad de actuar con autonomía relativa dentro de marcos doctrinales comunes. La preparación del personal, en consecuencia, debe formar operadores y comandantes capaces de comprender redes, dependencias, prioridades y efectos cruzados entre dominios (Hawley *et al.*, 2005; Priebe *et al.*, 2020; Serrano-Cuervo, 2026c). En este punto, la dimensión cognitiva del entrenamiento se vuelve tan importante como la técnica.

Otra implicación decisiva se refiere a la infraestructura crítica. La defensa multicapa multidominio obliga a redefinir qué se entiende por infraestructura estratégicamente protegible. Ya no se trata solo de bases aéreas, centros de comando o emplazamientos militares, sino también de redes eléctricas, telecomunicaciones, centros de datos, satélites, puertos, nodos logísticos y sistemas de transporte cuya afectación puede degradar gravemente la capacidad militar y la continuidad del Estado. La protección de infraestructura crítica deja así de ser un asunto periférico y pasa a ser parte constitutiva de la defensa. La literatura reciente sobre despliegue y proyección de fuerza en entornos multidominio subraya precisamente que sin protección de infraestructura crítica no hay sostenimiento efectivo de operaciones ni resiliencia nacional creíble (O'Brien, 2024; NATO, 2025; Serrano-Cuervo, 2026d). Esta comprobación obliga a una coordinación más estrecha entre defensa, gobierno, sector energético, telecomunicaciones y operadores de servicios esenciales.

Finalmente, la transición hacia una defensa multicapa multidominio transforma la toma de decisiones. La compresión del tiempo, la abundancia de datos y la simultaneidad de amenazas obligan a revisar las formas tradicionales de

decisión excesivamente jerárquicas o lentas. Los Estados y sus fuerzas armadas deberán equilibrar centralización estratégica con descentralización táctica, automatización con control humano, rapidez con confiabilidad y flexibilidad con disciplina doctrinal. Esto implica rediseñar procesos de mando y control, reglas de empuñamiento y esquemas de autoridad para que la defensa pueda actuar con velocidad sin perder coherencia ni legitimidad (Priebe *et al.*, 2020; Russell, 2019; Scharre, 2018). En un entorno multidominio, decidir tarde equivale con frecuencia a no decidir. Pero decidir rápido sin arquitectura adecuada puede amplificar errores sistémicos. La clave, por tanto, está en construir decisiones mejor informadas, distribuidas y resilientes.

En suma, las implicaciones estratégicas, operacionales y doctrinales de la defensa multicapa multidominio son profundas. Para los Estados, supone integrar la defensa en la estrategia nacional de disuasión y resiliencia. Para las fuerzas armadas, exige reorganizar operaciones, sostenimiento y mando bajo una lógica distribuida. Para la doctrina, demanda superar compartimentos heredados y articular funciones convergentes. Para el entrenamiento, obliga a formar operadores y mandos aptos para la complejidad. Para la infraestructura crítica, implica reconocer que la supervivencia del sistema depende de mucho más que sus interceptores. Y para la toma de decisiones, plantea la necesidad de combinar velocidad, inteligencia y control significativo.

Conclusiones

El trabajo de análisis que se ha realizado a lo largo de este capítulo reafirma, en efectividad, la tesis central propuesta: la respuesta adecuada a las amenazas contemporáneas debe surgir de la evolución hacia sistemas de defensa multicapa, integrados, adaptativos y multidominio. La ventaja defensiva en el ámbito estratégico, en la actualidad, dependerá menos de la posesión de un sistema singular, y más de la capacidad de articular sensores, mando y control, interceptores, redes, automatización, ciberresiliencia, convergencia entre dominios bajo una arquitectura coherente de defensa (Rozman, 2020; Stafford, 2021; IAMD CoE, 2023). Esta comprobación reafirma que el problema central ya no es únicamente cuál es el medio que tiene un Estado, sino cómo se integra y se adapta frente a unas amenazas simultáneas, distribuidas y cada vez más complejas.

En este sentido, la pregunta de investigación que ha guiado el capítulo ¿cómo deben evolucionar los sistemas de defensa multicapa en relación con las amenazas simultáneas para poder sobrevivir en los dominios aéreo, terrestre, marítimo, espacial y ciber? permite dar la clara respuesta de que deben evolucionar, para llegar al objetivo de la investigación. En primer lugar, doctrinalmente, avanzando a un enfoque de defensa multidominio, donde se busca la protección del espacio aéreo y la funcionalidad completa del sistema. En segundo lugar, operacionalmente, pasando a redes distribuidas, escalonadas y resilientes que sean capaces de mantener la coherencia a pesar de sufrir degradación parcial. En tercer lugar, tecnológicamente, integrando arquitectura abierta, interoperabilidad, fusión de datos de sensores, automatización supervisada, ciberresiliencia y modularidad como los medios de adaptación continua (Muravska, 2023; Priebe *et al.*, 2020; Serrano-Cuervo, 2026d). Igualmente, el examen del modelo clásico de la defensa antiaérea dio pie a identificar las razones por las que este resulta como insuficiente como respuesta única.

Se evidenció, además, que esta modificación es resultado de una mutación verificable del entorno estratégico. La amenaza contemporánea ha cambiado desde vectores relativamente diferenciados a otras configuraciones híbridas, atóricas, distribuidas y multiorigen, donde se mezclan drones, misiles, operaciones cibernéticas, guerra electrónica, plataformas espaciales, agentes estatales y no estatales y cada vez un marco de acceso más amplio a tecnologías directamente avanzadas (Serrano Cuervo, 2026a; Rogers & Kunertova, 2022; Jensen & Atalan, 2025). De esta manera, ya no se pueden encontrar puntos de organización con supuestos de linealidad, tiempos amplios para la decisión o separación tajante entre los dominios. La mutación de la amenaza se ajusta, por lo tanto, a una mutación correlativa de la defensa.

La inflexible rigidez doctrinal, la segmentación de los sensores, la dependencia de un mando jerárquico lento, así como la incapacidad para hacer frente a ataques simultáneos y distribuidos son evidencias de que la defensa tradicional fue pensada para un mundo menos interdependiente, menos rápido y denso que el actual (Hawley *et al.*, 2005; Corey, 2017; Stafford, 2021). El argumento de su obsolescencia no encuentra una excelente fundamentación, dado que no es tanta una obsolescencia absoluta sino de insuficiencia relativa con relación a una elevación en la escala del conflicto, la velocidad de este y la complejidad de este. Por ello, la necesidad de una evolución dirigida a una defensa multicapa

de múltiples dominios es entendida como una adaptación de los principios existentes a unas condiciones estratégicas nuevas y no como una ruptura arbitraria con el pasado.

En función de lo anterior, como primera recomendación conceptual que se puede ofrecer a los estudios estratégicos, sería la de dejar de lado lecturas en exceso atendidas a lo que está de moda que es la *platform-centric* o la *dominion-centric* del problema defensivo. La defensa multicapa debe situarse como un sistema de sistemas, como una arquitectura sociotécnica y como un problema de integración estratégica más que como simple sumatoria de armas o capas de interceptación. Todo ello implica incorporar marcos de análisis contemplados en la teoría de sistemas complejos, la interdependencia entre dominios y el análisis de redes funcionales, sin olvidar que la guerra es política y coercitiva (Serrano-Cuervo, 2026c; Freedman, 2019; Gray, 2015). Es decir, la aportación conceptual no implica sustituir la teoría de la guerra, sino enriquecerla para comprender mejor sus transformaciones de carácter.

Una segunda recomendación va dirigida al campo de la seguridad y de la defensa. La evolución de los sistemas multicapa exige considerar la protección de infraestructura crítica, la ciberresiliencia, la interoperabilidad institucional y la continuidad funcional del Estado como partes constitutivas de la defensa. La separación drástica entre defensa tradicional, ciberseguridad, protección de las infraestructuras críticas y la resiliencia nacional es cada vez más difícilmente sostenible en unos entornos que muestran cómo efectivamente la afectación de nodos digitales, energéticos o logísticos puede tener incluso efectos estratégicos que sean equivalentes y/o complementarios a los de un ataque cinético (NATO, 2025; O'Brien, 2024; Serrano-Cuervo, 2026d). Se deduce con ello que la defensa multidominio necesita un enfoque más holístico, donde militares y civiles puedan compartir criterios de prioridades, protección y respuesta.

La tercera recomendación hace referencia a la doctrina y la formación. Las fuerzas armadas deben revisar los marcos doctrinales, los ejercicios y los procesos de toma de decisiones para preparar a los operadores y a los mandos para actuar en redes, gestionar la incertidumbre, operar con información incompleta y sostener la defensa en condiciones degradadas. El entrenamiento ya no puede limitarse a la operación técnica de sistemas concretos, sino que es

necesario incluir saturación, disrupción cibernética, pérdida de sensores, confluencias de dominios, toma de decisiones como compresión temporal. Esto requiere una cultura de adaptación y aprendizaje institucional que reconozca la defensa multicapa como problema doctrinal, cognitivo y tecnológico (Priebe *et al.*, 2020; Scharre, 2018; Serrano-Cuervo, 2026c).

Por lo tanto, la eficacia futura de la defensa multicapa estará supeditada a su capacidad de ajustarse desde una lógica predominantemente antiaérea hacia una lógica genuinamente multidominio, lo que significa redefinir la defensa como red funcional de protección, detección, decisión, resiliencia y respuesta, en el que los dominios aéreo, terrestre, marítimo, espacial y ciber actúan de manera convergente. Para los estudios estratégicos, ello supone repensar categorías analíticas heredadas; para la seguridad y la defensa implica la combinación de resiliencia nacional, infraestructura crítica y arquitectura de defensa; y para la doctrina preparar organizaciones que sean capaces de adaptarse a un conflicto de más velocidad, más distribuidos, más tecnológicamente interdependientes. La defensa multicapa del futuro será sobre todo más integrada, abierta, resiliente e inteligente.

Referencias

- Almodovar, G., Allmacher, D. P., Ames III, M. P., & Davies, C. (2018). Joint Integrated Air and Missile Defense. Simplifying an Increasingly Complex Problem. *Joint Force Quarterly*, 88, pp. 78-84. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_78-84_Almodovar-et-al.pdf
- Boban, I. (2025). Requirements of Modern Air Defence. *Strategos*, 9(2), 11-36. <https://doi.org/10.65243/s.9.2.1>
- Boyd, J. (2018). *The essence of winning and losing*. Air University Press.
- Broch Hueso, J. (2012). La contribución del ET a la defensa antimisil. *Instituto Español de Estudios Estratégicos*. [Documento Marco]. https://www.ieee.es/Galerias/fichero/docs_marco/2012/DIEEEM12-2012_ContribucionETDefensaAntimisil_JBrochHUeso.pdf
- Chávez, F., & Swed, O. (2020a). Off the shelf: The violent nonstate actor drone threat. *Air & Space Power Journal*, 34 (3), pp. 29-43. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf

- Chavez, K., & Swed, O. (2020b). The proliferation of drones to violent nonstate actors. *Defence Studies*, 21(1), pp. 1-24. <https://doi.org/10.1080/14702436.2020.1848426>
- Clausewitz, C. von. (2007). *De la guerra* [trad. Castellana]. La Esfera de los Libros.
- Corey, C. R. (2017). The Air Force's misconception of integrated air and missile defense. *Air & Space Power Journal*, 31 (4), pp. 81-90. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-31_Issue-4/V-Corey.pdf
- Dahlgren, M., Bazylczyk, P., & Karako, T. (2025). *Mesh sensing for air and missile defense*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-07/250717_Dahlgren_Mesh_Sensing.pdf
- Davis, E. A. (2025). Drones and the Changing Character of War. *Parameters*, 55 (4), pp. 75-97. <https://press.armywarcollege.edu/parameters/vol55/iss4/7/>
- Davis, J. K. (2017). Development of system architecture to investigate the impact of integrated air and missile defense in a distributed lethality environment [Thesis of Master]. Naval Postgraduate School. <https://apps.dtic.mil/sti/trecms/pdf/AD1053193.pdf>
- Department of Defense. (2020). *Modular Open Systems Approach (MOSA) Reference Framework*. U. S. Department of Defense. <https://ac.cto.mil/wp-content/uploads/2020/06/MOSA-Ref-Frame-May2020.pdf>
- Dumitrescu, T. (2023). Adapting NATO's integrated air and missile defense to multi-domain operations. In *Proceedings of the International Scientific Conference Strategies XXI* [Vol. XIX]. National Defence University Publishing House. <https://www.ceeol.com/search/chapter-detail?id=1245500>
- Fox, A. (2021). Manoeuvre is Dead? Understanding the Conditions and Components of Warfighting. *The RUSI Journal*, 166 (6/7), pp. 10-18. <https://doi.org/10.1080/03071847.2022.2058601>
- Fox, A. (2026). Drones and land warfare: generating strategically relevant outcomes in conflict and war. *Defense & Security Analysis*, 1-21. <https://doi.org/10.1080/14751798.2026.2678663>
- Freedman, L. (2019). *La Guerra futura. Un estudio sobre el pasado y el presente*. Critica.
- Frenkel, G. (1994). *Flexible architectures for sensor fusion in theater missile defense*. Institute for Defense Analyses. <https://apps.dtic.mil/sti/html/tr/ADA288666/>

- Gady, F. S., & Stronell, A. (2020). Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030. In A. Ertan, K. Floyd, P. Pernik, T. Stevens (Eds.). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. CCDCOE NATO Cooperative Cyber Defence Centre of Excellence; King's College London; William & Mary. <https://www.ccdcoe.org/uploads/2020/12/8-Cyber-Capabilities-and-Multi-Domain-Operations-in-Future-High-Intensity-Warfare-in-2030.pdf>
- Gray, C. S. (2015). *The future of strategy*. Polity Press.
- Großwald Systems Desk. (2026). *Großwald Systems: Integrated Air and Missile Defense (IAMD)*. <https://www.grosswald.org/integrated-air-and-missile-defense-multilayer-architecture-from-shorad-to-strategic-shielding/>
- Gürsu, M. (2026). Lessons learned for air defence: the 2024 Iran-Israel "probing" warfare. *Defense & Security Analysis*, pp. 1-30. <https://doi.org/10.1080/14751798.2026.2658331>
- Hawley, J. K., Mares, A. L., & Giammanco, C. A. (2005). *The Human Side of Automation: Lessons for Air Defense Command and Control*. Army Research Laboratory. <https://apps.dtic.mil/sti/pdfs/ADA431964.pdf>
- Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
- Horowitz, M. C. (2018, April, 23). The promise and peril of military applications of artificial intelligence. *Bulletin of the Atomic Scientists*. <https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/>
- IAMD CoE. (2023). Integrated Air and Missile Defence: A valuable pillar in NATO's Deterrence and Defence. *IAMD CoE's Annual Journal*, 2. https://iamd-coe.org/wp-content/uploads/2023/11/IAMD_CoE_Journal_2023.pdf
- Jensen, B. & Atalan, Y. (2025, May). Drone saturation: Russia's Shahed Campaign. *CSIS Briefs*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-05/250513_Jensen_Drone_Saturations.pdf
- Jokinen, J., & Normark, M. (2022). *Hybrid threats from non-state actors: A taxonomy*. European Centre of Excellence for Countering Hybrid Threats. <https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf>

- Kunertova, D. (2023). The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin of the Atomic Scientists*, 79 (2), pp. 95-102. <https://doi.org/10.1080/00963402.2023.2178180>
- Maurer, D. E., Schirner, R. W., Kalandros, M. K., & Peri, J. S. J. (2006). Sensor Fusion Architectures for Ballistic Missile Defense. *Johns Hopkins APL Technical Digest*, 27(1), pp. 19-31. https://www.jhuapl.edu/techdigest/content/techdigest/pdf/V27-N01/27-01-Maurer_D.pdf
- Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict*. U.S. Army War College Press. <https://press.armywarcollege.edu/monographs/428/>
- Molina, A. C. (2025. September, 26). The point defense paradox: Sustaining airpower in contested environments. *Wild Blue Yonder*. Air University. <https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/4316568/the-point-defense-paradox-sustaining-airpower-in-contested-environments/>
- Morin, E. (1990). *Introducción al pensamiento complejo*. Gedisa. https://redpaemigra.weebly.com/uploads/4/9/3/9/49391489/morin_introduccion_al_pensamiento_complej.pdf
- Moulton, C. L., Krzywicki, A. T., Hepp, J. J., Harrell, J., & Kogut, M. (2015). Open architecture design and approach for the Integrated Sensor Architecture (ISA). *Proceedings*, 9479. <https://doi.org/10.1117/12.2177842>
- Muravska, J. (2023). *European Integrated Air and Missile Defence in NATO: Progress and Persistent Challenges*. Freeman Air & Space Institute; King's College London. <https://www.kcl.ac.uk/warstudies/assets/paper-16-julia-muravska-european-integrated-air-and-missile-defence.pdf>
- NATO. (2025. February, 13). *NATO Integrated Air and Missile Defence Policy*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy>
- O'Brien, M. (2024. June, 20). Protection of Critical Infrastructure in Support of the Deployment of U.S. Forces During Multidomain Operations. *Homeland Defense & Security Information Analysis Center*. <https://hdiac.dtic.mil/articles/protection-of-critical-infrastructure-in-support-of-the-deployment-of-u-s-forces-during-multidomain-operations/>

- Pietrus, T. (2023). IAMD (Integrated Air and Missile Defense) Strategic Aspects with SBAD Focus. *Safety & Defense*, 9(1), pp. 69-73. <https://doi.org/10.37105/sd.200>
- Priebe, M., Ligor, D.C., McClintock, B., Spirtas, M., Schwindt, K., Lee, C., Rhoades, A. L., Eaton, D., Hodgson, Q. E., & Rooney, B. (2020). *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA381-1/RAND_RRA381-1.pdf
- Rauta, V. (2019). Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. *Cambridge Review of International Affairs*, 33(6), pp. 868-887. <https://doi.org/10.1080/09557571.2019.1656600>
- Rehberg, C., & Kemp, H. (2023). *Strengthening the phalanx: Layered, comprehensive, and distributed air and missile defense in the Indo-Pacific*. Center for Strategic and Budgetary Assessments. <https://csbaonline.org/research/publications/strengthening-the-phalanx-layered-comprehensive-and-distributed-air-and-missile-defense-in-the-indo-pacific>
- Reilly, J. M. (2016). Multidomain Operations: A Subtle but Significant Transition in Military Thought. *Air & Space Power Journal*, 30 (1), pp. 61-73. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-1/V-Reilly.pdf
- Rogers, J., & Kunertova, D. (2022). *The vulnerabilities of the drone age: Established threats and emerging challenges*. Center for War Studies; ETH Zürich CSS; The NATO Science for Peace and Security Programme. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO_VDA_Policy_Report.pdf
- Rozman, J. (2020). Integrated Air and Missile Defense in Multi-Domain Operations. *Spotlight*, 20(2), 1-12. <https://indianstrategicknowledgeonline.com/web/integratedairandmissiledefenseinmultidomainoperations.pdf?view=1>
- Russell, S. (2019). *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking.
- Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company.
- Serrano Cuervo, A. (2026a). La transformación del carácter de la guerra en el siglo XXI: Guerra híbrida, tecnología y amenazas emergentes en América Latina y Colombia. En A. Serrano Cuervo & G. E. Narváez Jaimes (Eds.), *Seguridad integral y resiliencia nacional: Preparación estratégica ante amenazas con-*

- temporáneas* (pp. 15-60). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818781.01>
- Serrano-Cuervo, A. (2026b). La naturaleza y el carácter de la guerra: Del pensamiento estratégico clásico a las guerras híbridas. En D. López Niño & A. Serrano-Cuervo (Eds.), *Teoría de la guerra y liderazgo estratégico en los conflictos contemporáneos* (pp. 5-30). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818743.01>
- Serrano-Cuervo, A. (2026c). El salto cuántico del conocimiento estratégico: Nuevas epistemologías para los sistemas militares complejos. En O. O. Porras-Rodríguez & A. Serrano-Cuervo (Eds.), *Educación militar y pensamiento complejo: Epistemología, liderazgo y transformación curricular en la Escuela Superior de Guerra* (pp. 179-207). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818538.07>
- Serrano-Cuervo, A. (2026d). Innovación y adaptación: Capacidades militares frente a amenazas emergentes en la guerra tecnológica contemporánea. En M. E. Realpe-Díaz & A. M. González-González (Eds.), *Transformación digital y ciberseguridad en Colombia: Desafíos estratégicos para sectores de infraestructura crítica* (pp. 69-118). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818644.03>
- Singh, T. (2024). Evolution of Multi-Domain Operations and Prospects for Application of Aerospace Power. *Journal of Defence Studies*, 18(1), 67-87. https://www.idsa.in/wp-content/uploads/2024/05/18-1_Tejinder-Singh.pdf
- Stafford, J. C. (2021). Multidomain Ready: How Integrated Air and Missile Defense Is Leading the Way. *Joint Force Quarterly*, 100(1), pp. 101-106. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-100/jfq-100_101-106_Stafford.pdf
- Topor, S., Vevera, V., Georgescu, A., & Ciuperca, E. M. (2025). Artificial intelligence in multidomain operations: A SWOT analysis. *Bulletin of "Carol I" National Defence University*, 14(1), 108-121. <https://doi.org/10.53477/2284-9378-25-07>
- U.S. Air Force. (2025). Air Force Doctrine Publication 3-0, Operations. *AFDP 3-0, Operations*. United States Air Force. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-0/AFDP3-0Operations.pdf
- U.S. Navy & U.S. Marine Corp. (2025). *Naval Modular Open System Approach Guidebook*. U.S. Navy. <https://www.cto.mil/wp-content/uploads/2025/05/Naval-MOSA-Implementation-Guide-V1.0.pdf>

- van Hooft, P., & Boswinkel, L. (2021). *Surviving the Deadly Skies: Integrated Air and Missile Defence 2021–2035*. The Hague Centre for Strategic Studies. <https://hcss.nl/wp-content/uploads/2021/12/Integrated-Air-and-Missile-Defense-HCSS-Dec-2021.pdf>
- Vogler, K. I., Brown, M. J., Fass, R. D., Lucas, B. M., & Ritschel, J. D. (2026). Modular Open Systems Approach. Impacts on Program Management Metrics. *Defense ARJ*, 33 (1), pp. 2-28. <https://doi.org/10.22594/dau.24-933.33.01>
- Wirtz, J. J. (2019). A New Agenda for Security and Strategy? En Baylis, J., Wirtz, J. J., & Gray, C. S. *Strategy in the contemporary world: An introduction to strategic studies* [pp. 366-384] (6th ed.). Oxford University Press. <https://robertedwinkelly.com/wp-content/uploads/2022/02/strategy-in-the-contemporary-world-6e.pdf>



CAPITULO CUARTO

ECUADOR, ACADEMIA DE DEFENSA MILITAR CONJUNTA (ADEMIC)

La influencia de las nuevas tecnologías en los escenarios de operaciones frente a las amenazas híbridas y crimen organizado transnacional: una perspectiva

Luis Fernando Pillajo

Resumen: El presente artículo analiza la influencia de las nuevas tecnologías, particularmente la inteligencia artificial (IA), en la configuración de los escenarios operacionales frente a amenazas híbridas y crimen organizado transnacional. Se identifica como problemática central la brecha entre la acelerada evolución tecnológica y las capacidades institucionales del Estado. Desde un enfoque teórico y mediante análisis documental, queda claro que la inteligencia artificial está transformando los escenarios de conflicto, extendiendo las capacidades operativas en contextos multidominio. Concluye que el Estado se enfrenta a un contexto de alta complejidad estratégica que exige la integración de capacidades estatales, el fortalecimiento de la gobernanza tecnológica y una visión prospectiva de la seguridad nacional.

Palabras clave: Inteligencia artificial, multidominio (tierra, aire, ciberespacio, información), amenazas híbridas, crimen organizado, seguridad integral.

Acerca del autor: Coronel **Luis Fernando Pillajo**, militar en servicio activo del Ejército del Ecuatoriano cumple, actualmente la función de director de la Academia de Defensa Militar Conjunta, ha realizado estudios de en Seguridad, Defensa y Desarrollo, participando en diversos eventos académicos, lo que le ha permitido alcanzar una perspectiva de la realidad en los diferentes niveles.

lfpillajog@ejercito.mil.ec.

Academia de Defensa Militar Conjunta, Quito – Ecuador

Introducción

El entorno estratégico actual está marcado por una transformación estructural impulsada por el desarrollo tecnológico, la digitalización y la globalización. En este contexto, las amenazas tradicionales han evolucionado hacia formas complejas y multidimensionales, destacando las amenazas híbridas y el crimen organizado transnacional, que han adquirido una relevancia creciente debido a que combinan distintas formas de presión, conflicto y desestabilización, lo que exige otras capacidades de análisis y respuesta por parte de los Estados. Bartolomé (2019), afirma que la hibridación puede entenderse tanto como la acción de actores que emplean modos de combate híbridos como la combinación sinérgica de al menos dos amenazas diferentes, lo que ha ampliado el campo de acción de la seguridad internacional y sus manifestaciones.

Las amenazas contemporáneas ya no se limitan al plano militar tradicional, sino que incluyen fenómenos como el narcotráfico, el crimen organizado, la delincuencia y los riesgos cibernéticos, en este contexto Barriga Carrera (2022) sostiene que las amenazas multidimensionales y las amenazas híbridas se expanden en un contexto globalizado y tienen efectos en los ámbitos político, social y económico, además de proyectarse al ciberespacio.

El modelo actual de seguridad deberá busca un enfoque integral para articular los diferentes niveles de acción del Estado, tomando en cuenta la interacción entre factores políticos, económicos, tecnológicos y sociales.

El entorno de seguridad ya no es exclusivamente militar, sino multidimensional e interconectado, sustentado en la actual transición hacia un contexto de seguridad compleja y amenazas globalizadas, donde los Estados enfrentan desafíos

que superan sus capacidades tradicionales. Las amenazas no convencionales y los actores no estatales exigen una transformación de las Fuerzas Armadas y de las capacidades del Estado, así como una formación académica especializada para enfrentar un entorno en el que las capacidades estatales pueden verse desbordadas (Grae. Paco M., 2024).

Desde esta nueva realidad, analizar la influencia de las nuevas tecnologías en los escenarios de operaciones frente a las amenazas híbridas y al crimen organizado transnacional permite abordar en la actualidad un problema estratégico, al cual convergen la transformación de los conflictos, la innovación tecnológica y la mutación de los actores ilícitos. Este acercamiento resulta pertinente para el caso ecuatoriano, donde la dinámica de la violencia ha sido vinculada de acuerdo con su accionar por el crimen organizado de alcance transnacional y a la evolución de las economías ilícitas (Escobar-Jiménez, 2024).

El incremento de la violencia asociada al crimen organizado y la creciente digitalización de las amenazas configuran un escenario de alta complejidad, donde la inteligencia artificial emerge como un factor determinante, dentro de un sistema internacional caracterizado por incertidumbre, interdependencia y transformación tecnológica. (Grae. Paco M., 2024).

Desde una perspectiva estratégica se deberá analizar la influencia de las nuevas tecnologías en los escenarios de operaciones frente a amenazas híbridas y crimen organizado transnacional.

Marco teórico

Estrategia y multidimensionalidad del conflicto

La estrategia contemporánea debe ser comprendida como un proceso dinámico orientado a la toma de decisiones en entornos complejos. En este sentido, desde una perspectiva clásica, la guerra y su conducción han sido entendidas como instrumentos fundamentales del poder del Estado, donde la organización, la disciplina y la preparación resultan determinantes para alcanzar la victoria (Maquiavelo, 2003).

Según A. Beaufre (1963), la estrategia no es un conjunto de reglas fijas, es un método flexible para analizar situaciones problemáticas, clasificar y jerarquizar factores y además elegir medios más adecuados según el escenario, existiendo formulas universales aplicables a cada caso, por lo que, cada situación estratégica (conflicto) necesita una estrategia que integre medios y objetivos adaptados al entorno, a los actores involucrados y los objetivos perseguidos; además establece dos grandes modos de estrategias, la primera la estrategia directa con el empleo principal de la fuerza militar que busca la decisión mediante la confrontación y la segunda la estrategia indirecta que instaura el uso predominante de medios no militares que busca debilitar gradualmente la voluntad del adversario, empleando la presión política, la influencia psicológica, económica y de información (propaganda); reafirmando que en el contexto contemporáneo, la guerra y la seguridad se desarrollan en múltiples dimensiones: política, económica, diplomática, psicológica y militar, constituyéndose en multidimensional y sistemática, de manera similar Liddell Hart (1967) sostiene que la aproximación indirecta busca desorganizar el equilibrio físico y psicológico del adversario mediante maniobras estratégicas que eviten la confrontación directa concepto que para esa época no consideró las dimensiones como la economía, la diplomacia y la información.

Posteriormente, **André Beaufre** propone una pirámide estableciendo la estrategia total (conducción política del Estado), estrategia general (coordinación multisectorial de los recursos nacionales) y estrategia operativa (ejecución de acciones concretas) cuya propósito ideal es el alcanzar la victoria sin combate directo o con el menor costo posible, manteniendo como principios esenciales la capacidad de decidir bajo la presión del adversario (libertad de acción) y el uso eficiente de los recurso (economía de medios). Este planteamiento se inserta en el planteamiento de Carl Von Clausewitz, que concibió que “La guerra no es meramente un acto político, sino un verdadero instrumento político, una continuación de las relaciones políticas llevada a cabo por otros medios” priorizando la primacía del objetivo político en la conducción estratégica (Clausewitz, 1832/1989), sin embargo Clausewitz centra su análisis en la guerra interestatal y en el uso predominante de la fuerza militar, manteniendo un enfoque más estructurado en torno a principios como la concentración de fuerzas y la batalla decisiva, lo cual es rechazado por André Beaufre enfatizando la necesidad de la adaptación constante.

En esta perspectiva se puede conceptualizar que la guerra híbrida coincide en que los conflictos actuales se caracterizan por la convergencia de medios convencionales, irregulares, cibernéticos e informacionales, en este sentido Weissmann *et al.* (2021) definen la guerra híbrida como una estrategia que mezcla guerra convencional, guerra irregular, ciberataques y otros métodos de influencia, como la desinformación, la diplomacia y la intervención política, lo que obliga a repensar las categorías tradicionales de la estrategia (Weissmann *et al.* 2021).

A la actual transformación se debe sumar el efecto de las tecnologías conectadas sobre la forma de conducir la guerra, en este sentido Ford (2024) plantea que la guerra en Ucrania se desarrolla en una ecología informativa totalmente conectada, donde dispositivos cotidianos como los teléfonos inteligentes permiten geolocalizar columnas enemigas, controlar drones y difundir evaluaciones de daños, expandiendo la participación tanto de militares como de civiles en el desarrollo del conflicto (Ford, 2024).

En esta realidad, el desarrollo de la inteligencia artificial introduce cambios relevantes en la planificación y la toma de decisiones militares. Suleymanli y Hajiyev (2024) asevera que la integración de la inteligencia artificial influye en las operaciones militares al transformar las estrategias de combate, los procesos de decisión y el papel de la intervención humana en la guerra contemporánea (Suleymanli & Hajiyev, 2024); en este mismo sentido, Adler (2025) sostiene que, en un entorno de operaciones cada vez más acelerado, la velocidad en la toma de decisiones puede convertirse en un factor decisivo, por lo que la integración de IA en la planificación militar representa una necesidad de modernización institucional (Adler, 2025).

Las acciones del crimen organizado se pueden explicar mediante la estrategia indirectas, en donde evita la confrontación directa con el Estado, y busca la erosión de las instituciones, el influir en las decisiones políticas y el control de territorios en forma gradual en donde se puede comprender que las nuevas tecnologías se constituyen en su medio y amplificador del poder con bajo costo como ejemplo se puede mencionar los ciberataques, la desinformación y las redes sociales

En este tejido de crítico, el Estado debe orientar su acción hacia la estrategia total, es decir hacia la multidimensionalidad, las operaciones interagenciales y

el enfoque integral, trasladado al Estado se debe comprender el empleo de las Fuerzas Armadas, Policía Nacional, Inteligencia, Sistema Judicial y la Política Pública manteniendo una visión sistemática del poder nacional y de su empleo coordinado en escenarios de conflicto en donde la lucha se orienta a alcanzar la decisión mediante la creación de condiciones favorables que conduzcan a la desintegración moral del adversario es decir la pérdida de la voluntad de confrontación y su percepción mediante la aplicación de campañas de desinformación, control narrativo, legitimidad del Estado, proyectando su capacidad y voluntad.

Durante el desarrollo de los conflictos híbridos se evidencia la combinación de medios convencionales y no convencionales, en los cuales el uso de herramientas tecnológicas pasa a ser un elemento central.

En los modelos conceptuales sobre amenazas híbridas destacan la interacción de múltiples actores, herramientas y dominios, lo que genera escenarios operacionales altamente dinámicos y difíciles de predecir. Giannopoulos, G., *et al.* (2021).

Seguridad integral y amenazas contemporáneas

El concepto de seguridad ha evolucionado, desde una perspectiva exclusivamente centrada en la defensa militar, hacia enfoques más amplios e integrales. En esta misma línea Sisco Marcano y Chacón Maldonado (2004), enfatizan que la agenda de seguridad se amplía para incluir sectores económicos, sociales y ambientales, además de los ámbitos políticos y militares, lo que permite entender mejor la complejidad del entorno contemporáneo (Sisco Marcano & Chacón Maldonado, 2004).

Con una perspectiva complementaria, Peña-Galindo (2026) define la seguridad integral como un paradigma que trasciende la mirada estrictamente militar y articula dimensiones políticas, económicas, sociales, ambientales, tecnológicas y territoriales, con este enfoque resulta útil, el estudiar amenazas complejas, ya que incorpora la gobernanza, la coordinación institucional y la participación de distintos actores en el diseño de respuestas estratégicas (Peña-Galindo, 2026).

Las amenazas actuales, son fenómenos como el crimen organizado transnacional, la ciberdelincuencia y las operaciones de desinformación que afectan la estabilidad de los Estados. Así el crimen organizado transnacional presenta una estructura organizada, con capacidad para operar en varios países y orientación a la obtención de beneficios económicos ilícitos (Organización de las Naciones Unidas, 2004).

El crimen organizado transnacional, en particular, es una amenaza significativa, operando a través de redes globales que trascienden fronteras y debilitan las capacidades institucionales de los Estados, exigiendo respuestas coordinadas a nivel internacional.

Estas amenazas se producen al mismo tiempo en distintos ámbitos, creando un entorno de inseguridad sumamente complejo, que exige respuestas integradas.

En Ecuador como en toda la región, las amenazas contemporáneas se vinculan con el crimen organizado y fenómenos transnacionales ([Memorias XVII Seminario Online del Acdia Ecuador](#), 2026).

Colmenares-Zapata (2025) identifica cinco amenazas prioritarias que inciden de forma sinérgica sobre el bienestar económico, social, político y ambiental: el crimen organizado transnacional, la crisis climática, las migraciones forzadas, los riesgos cibernéticos y las pandemias. A partir de ello, el autor propone que los marcos tradicionales de seguridad centrados en el Estado resultan insuficientes y que se requieren respuestas integrales orientadas a la protección de las personas (Colmenares-Zapata, 2025).

El Ecuador adopta un enfoque de seguridad integral que articula defensa, seguridad pública y desarrollo (MDN del Ecuador, Plan Nacional de Seguridad Integral 2025–2029) sin embargo, enfrenta desafíos derivados del crimen organizado transnacional, narcotráfico, violencia estructural y amenazas digitales.

Dominio de la información y guerra cognitiva

El dominio de la información y la guerra cognitiva no son cosas que sucedan de manera aislada. En realidad, son la evolución natural de los principios estratégicos clásicos, pero adaptados a un mundo globalizado con mucha tecnología.

Los expertos en estrategia militar establecen que, aunque los medios han cambiado, la esencia del conflicto sigue siendo la misma.

Según la perspectiva de Clausewitz (1832/1989), la guerra es la continuación de la política, pero por otros medios. Esto representa que el objetivo final es influir en la voluntad del adversario. La guerra cognitiva es una forma lógica de aplicar este principio, pero se usa el control de la información y la manipulación de la percepción en lugar la fuerza física. Esto permite intervenir directamente en el proceso de toma de decisiones del adversario.

Liddell Hart (1967), también indica que es importante aplicar un enfoque indirecto para debilitar al adversario evitando enfrentarlo directamente. Esto se aplicará perfectamente a la guerra cognitiva, donde usando operaciones de información, desinformación y campañas psicológicas se puede lograr desestabilizar al oponente sin necesidad del combate directo. Las amenazas híbridas siguen esta lógica, ya que combinan herramientas militares y no militares para alcanzar los objetivos estratégicos.

En la actualidad, la incorporación de tecnologías emergentes ha cambiado radicalmente la forma de llevar a cabo estas dinámicas. Las redes sociales, el Big Data y la inteligencia artificial permiten a los actores influir en grandes audiencias y crear campañas de desinformación muy efectivas. Pillajo y Narváez (2022) establecen que el dominio de la información se traduce en la capacidad de manipular percepciones, influir en emociones y orientar comportamientos colectivos, lo que es fundamental en los conflictos actuales.

La aplicación de operaciones de información integra capacidades como las operaciones psicológicas, la ciberdefensa, la guerra electrónica y la comunicación estratégica, permitiendo alcanzar la superioridad informacional sobre el adversario. Estas capacidades se potencian con el uso de tecnologías digitales facilitando la difusión masiva e inmediata de contenidos, amplificando el impacto de las estrategias de influencia.

En esta trama, la guerra cognitiva es una de las principales manifestaciones de la guerra de quinta generación, caracterizada por el desplazamiento del conflicto hacia el dominio de la percepción y la mente humana. Buscando afectar la racionalidad del adversario, debilitar su cohesión social y generar condiciones

de inestabilidad política, manipulando herramientas como la propaganda, la desinformación y la manipulación mediática.

En la región, la guerra cognitiva es especialmente relevante debido a la utilización de la información como instrumento de influencia política y social. La presencia de actores en redes sociales, campañas mediáticas y estructuras organizadas de desinformación muestra que la guerra cognitiva es una realidad en el ámbito nacional. Según Pillajo y Narváez (2022), esto refleja la necesidad de fortalecer las capacidades del Estado para gestionar el entorno informacional y proteger a la población frente a la manipulación de la información.

Así las amenazas híbridas y el crimen organizado transnacional operan en escenarios complejos, donde el uso de herramientas informacionales y tecnológicas permite a diversos actores influir en la percepción social, debilitar la institucionalidad y generar condiciones de inestabilidad, en este sentido el ciberespacio, las redes sociales y las operaciones de información se constituyen en nuevos espacios de confrontación, en los que se disputa el control de la narrativa y la legitimidad del poder.

Metodología

Las amenazas híbridas y el crimen organizado transnacional han sido abordadas con frecuencia desde enfoques cualitativos, explicativos y documentales, es así que Cuervo Ceballos (2018), al analizar el crimen organizado transnacional en la Triple Frontera, emplea una metodología cualitativa, explicativa, analítica y documental para identificar los factores que favorecen el asentamiento de redes criminales y su carácter híbrido (Cuervo Ceballos, 2018).

En forma análoga, Visceglie (2022) propone una aproximación geopolítica para distinguir similitudes y diferencias entre la amenaza híbrida del terrorismo y el crimen organizado transnacional en espacios fronterizos latinoamericanos, con especial atención a la convergencia entre organizaciones criminales y las vulnerabilidades derivadas de respuestas estatales diferenciadas (Visceglie, 2022).

Fundamentada en las referencias presentadas, una metodología de revisión documental y análisis cualitativo nos resulta pertinente para examinar los

escenarios de operaciones frente a las amenazas híbridas y crimen organizado transnacional, ya que de esta manera se permite integrar aportes teóricos sobre seguridad y tecnología con los estudios centrados en la evolución de la criminalidad organizada y las transformaciones operacionales recientes.

Resultados y discusión

Se evidencia que las dinámicas tradicionales de la seguridad han sido superadas por un entorno caracterizado por la convergencia de amenazas híbridas, el uso intensivo de tecnologías emergentes y la creciente incidencia del crimen organizado transnacional; en este contexto, el dominio de la información se posiciona como un eje estratégico que permite a los distintos actores influir en la percepción social, alterar procesos de toma de decisiones y generar condiciones de inestabilidad política y social, en donde el control del entorno informacional resulta tan decisivo como el empleo del poder militar convencional

Transformación de los escenarios operacionales

La era de las tecnologías emergentes está modificando de forma sustantiva los escenarios operacionales. Ford (2024) muestra que la conectividad transforma la conducción de la guerra al insertar tanto actores civiles y militares dentro de una misma red de sensores, información y comunicaciones, donde los dispositivos cotidianos pueden adquirir funciones tácticas y operativas (Ford, 2024).

Los resultados evidencian el impacto de las nuevas tecnologías en los escenarios operacionales y en la conducción de operaciones militares y de seguridad, que han evolucionado hacia un entorno multidominio caracterizado por la integración de:

- Espacio físico
- Ciberespacio
- Entorno informacional

Influenciados por la tecnología

- Inteligencia artificial (IA)
- Vigilancia y
- Ciberdefensa

[Atkinson, R. (2025)].

La inteligencia artificial ha transformado la conducción de los conflictos armados (Atkinson, R. (2025); al operar tanto como medio es decir mediante sistemas autónomos y como método, sustancialmente en la toma de decisiones y operaciones psicológicas, lo que amplía el alcance de las amenazas híbridas que integra las dimensiones militares, psicológicas e informacionales en escenarios multidominio (Matiz & Fernández, 2023, pp. 524–526).

En la esfera de la planificación militar, Adler (2025) sostiene que la inteligencia artificial puede contribuir a mejorar la comprensión del entorno operacional, el desarrollo de cursos de acción y la velocidad de respuesta, aunque también plantea desafíos asociados a la adaptación doctrinal y a la integración de estas capacidades en marcos tradicionales de planeamiento (Adler, 2025). Con una perspectiva complementaria Suleymanli y Hajiyevev (2024) establece que la IA no solo modifica procedimientos tácticos, sino también las formas de razonamiento ligadas al conflicto y a la conducción de operaciones (Suleymanli & Hajiyevev, 2024)

En este contexto, se puede afirmar, que la inteligencia artificial introduce nuevas capacidades permitiendo optimizar el procesamiento de información, la toma de decisiones y la planificación estratégica (Atkinson, R. (2025); sin embargo, estas capacidades también son utilizadas por el crimen organizado transnacional (COT), que también puede adoptar estas tecnologías como método operativo para optimizar sus actividades ilícitas.

Partiendo de la literatura mostrada sobre amenazas contemporáneas y el uso de tecnologías emergentes, se presenta el resumen de su tipología:

Tipo de amenazas	Nivel de uso tecnológico	Características tecnológicas	Impacto estratégico
Crimen organizado transnacional	Alto	Redes digitales, criptografía, logística IA	Alto
Amenazas híbridas	Muy alto	Desinformación, ciberataques, IA	Crítico
Ciberdelincuencia	Extremo	Malware, hackeo, automatización	Crítico

Tabla 1. Tipología de amenazas y uso de tecnología. Fuente: Elaboración propia con base en ONU (2004), Rodríguez *et al.* (2023), Atkinson (2025) y Matiz & Fernández (2023).

Se puede determinar que las amenazas contemporáneas el crimen organizado transnacional, amenazas híbridas y la ciberdelincuencia presentan un alto nivel de dependencia tecnológica, determinando que la ciberdelincuencia actual posee un nivel de uso tecnológico extremo mediante malware, hackeo y automatización constituyendo un impacto estratégico crítico para el Estado.

Capacidad IA	Aplicación en defensa	Aplicación en crimen organizado
Análisis de datos	Inteligencia estratégica	Análisis de rutas ilícitas
Automatización	Sistemas autónomos	Operaciones digitales
Predicción	Anticipación de amenazas	Optimización criminal
Procesamiento de datos	Vigilancia e inteligencia	Evasión de control estatal

Tabla 2. Capacidades de la inteligencia artificial en seguridad Fuente: Elaboración propia con base en (Atkinson, R. (2025).

A partir de los planteamientos sobre escenarios multidominio se presenta la siguiente tipología:

Dominio	Características principales	Ejemplo en Ecuador
Físico	Inteligencia estratégica	Análisis de rutas ilícitas
Ciberspacio	Sistemas autónomos	Operaciones digitales
Informacional	Anticipación de amenazas	Optimización criminal

Tabla 3. Escenarios operacionales multidominio Fuente: Elaboración propia con base en Matiz & Fernández (2023), Atkinson (2025) y Rodríguez *et al.* (2023).

Impacto en amenazas híbridas

Las transformaciones tecnológicas y su impacto debe analizarse también en relación con las amenazas híbridas, con esta visión Góngora Montejano (2025) plantea que, a partir de la transnacionalización de la delincuencia organizada y de la posibilidad de afectar infraestructuras críticas, emerge un fenómeno complejo de hibridación entre terrorismo y delincuencia organizada, especialmente visible en espacios de “zonas grises” donde no existe guerra declarada, pero tampoco ausencia de conflicto (Góngora Montejano, 2025).

A partir de un punto de vista más amplio, Long (2025) explora cómo el crimen organizado consigue converger con acciones encubiertas e irregularidad estratégica, exponiendo que la articulación entre redes criminales y objetivos de poder puede erosionar la legitimidad de los Estados y generar ventajas en contextos de confrontación híbrida (Long, 2025).

En este sentido, se debe considerar que las amenazas híbridas integran dimensiones militares, psicológicas e informacionales y utilizan herramientas no convencionales como:

- Desinformación digital
- Guerra cognitiva
- Ciberataques
- Manipulación social
- Uso de tecnologías como IA para la desinformación (Rodríguez *et al.*, 2023).

Estas características robustecen la complejidad del conflicto contemporáneo.

Crimen organizado transnacional

El crimen organizado transnacional ha sufrido una transformación importante en las últimas décadas, pasando de estructuras jerárquicas tradicionales a modelos organizativos más flexibles y dinámicos, caracterizados por redes descentralizadas con alcance regional y mundial, y estas organizaciones han ampliado sus actividades más allá del tráfico de drogas, incorporando delitos como el tráfico de personas, el lavado de activos, el cibercrimen y la minería ilegal, lo que demuestra su capacidad de adaptación ante los cambios del en-

torno internacional. Aquí es donde el crimen organizado trasciende las fronteras estatales, aprovechando la globalización, las debilidades institucionales y las brechas de gobernanza para afianzar su presencia en múltiples territorios. Esta evolución ha transformado al crimen organizado en un actor con capacidades comparables, en algunos aspectos, a las de los Estados, en especial a lo relacionado con control de territorios, generación de recursos económicos y su influencia sobre estructuras políticas y sociales.

El crimen organizado utiliza tecnologías emergentes para:

- Patrocinar estructuras flexibles y expandir sus redes globales
- Propagar sus operaciones
- Robustecer su capacidad operativa
- Adaptarse en entornos digitales y vincularse con conflictos híbridos

El uso de tecnologías como la encriptación y las plataformas digitales ha renovado la eficiencia operativa de las organizaciones criminales, permitiéndoles evitar controles estatales y mantener altos niveles de anonimato. Luvecce Ramírez, R. (2024).

Este fenómeno acrecienta la dificultad del control por parte del Estado.

En la región, el narcotráfico y crimen organizado generan un escenario de violencia con características híbridas ([260520 Rev. MEMORIAS XVII SEMINARIO ONLINE DEL ACIDIA ECUADOR](#)). El incremento de la violencia no puede entenderse únicamente desde factores internos, sino también desde la inserción del Estado en dinámicas transnacionales del crimen organizado. Escobar-Jiménez (2024), estableciendo una explicación multifactorial del aumento de la violencia señalando que esta debe analizarse desde la estructura general de las economías ilícitas y desde la relación entre los problemas globales y locales (Escobar-Jiménez, 2024).

El Observatorio Ecuatoriano de Crimen Organizado (OECO, 2025) indica que el panorama criminal en Ecuador ha experimentado cambios significativos, caracterizados por una mayor diversificación y fragmentación de la criminalidad. Además, el informe señala el crimen organizado ha evolucionado hacia una estructura más fragmentada y diversificada, donde diferentes grupos operan en múltiples mercados ilícitos al mismo tiempo, se evidencia una profesionali-

zación de las actividades criminales, observada en la organización de las redes y en el control territorial que ejercen (OECD, 2025).

Uso de información y desinformación

La información y la desinformación estimuladas por la IA se convierten en una herramienta estratégica para el crimen organizado, estos actores las usan en campañas informativas, manipulación mediática y redes sociales para cimentar narrativas a favor de sus intereses, transgredir en la percepción de la población y debilitar la legitimidad de las instituciones estatales (Pillajo & Narváez, 2022).

El crimen organizado, además, utiliza el ciberespacio lo que permite que estas organizaciones desarrollen actividades como el cibercrimen, el espionaje digital y la difusión de contenidos ilícitos, ampliando sus operaciones más allá del ámbito físico. La convergencia de violencia, tecnología y manipulación informacional conforma un complejo escenario en el que el crimen organizado no solo significa una amenaza delictiva, sino además un actor estratégico dentro de los conflictos híbridos.

Conclusiones

- La tecnología, especialmente la IA, redefine los conflictos y las amenazas, constituyendo un factor disruptivo en la seguridad y defensa contemporánea.
- Los desafíos éticos y jurídicos del empleo de la IA en los conflictos armados demanda la necesidad de fortalecer el derecho internacional, específicamente en lo relacionado con el control humano, la responsabilidad y la regulación de sistemas autónomos.
- Los escenarios de conflicto van evolucionando hacia entornos multidominio y tecnológicamente intensivos.
- Las amenazas híbridas y el crimen organizado transnacional muestran una alta capacidad de adaptación tecnológica.
- Las amenazas híbridas y el crimen organizado demandan respuestas multidimensionales.

- Se requiere fortalecer la seguridad integral del Estado a través de la integración institucional y la cooperación internacional por lo que la adaptación doctrinal es fundamental para enfrentar estos desafíos.
- Las Fuerzas Armadas tienen que evolucionar hacia modelos más flexibles, tecnológicos y colaborativos.
- La planificación estratégica y prospectiva es fundamental para anticipar y gestionar amenazas futuras.
- El Estado requiere una política integral y estructurada para la gestión estratégica de la información, sin embargo al no disponerla representará una debilidad institucional que dificulta la capacidad para contrarrestar las campañas de desinformación y proteger a la población frente a la manipulación informativa.
- El dominio de la información y la guerra cognitiva exige la adaptación de los Estados y sus instituciones hacia enfoques integrales que consideren tanto la dimensión militar como el dominio informacional y cognitivo del conflicto.
- La formación académica especializada en seguridad y defensa es clave para fortalecer las instituciones públicas.
- La seguridad contemporánea requiere un enfoque sistémico que integre tecnología, gobernanza, cooperación internacional y desarrollo institucional. La articulación de estos elementos permite comprender que las amenazas híbridas y el crimen organizado transnacional no solo representan riesgos operativos, sino también desafíos estructurales para el Estado, que demandan respuestas coordinadas y sostenibles en el tiempo.

Referencias

- Adler, J. N. (2025). Modernizing military decision-making: Integrating AI into Army planning. *Military Review*.
- Aharonian, A. (2018, 4 de septiembre). Guerra de quinta generación. *La Tinta*. <https://latinta.com.ar/2018/09/guerra-quinta-generacion/>
- Atkinson, R. (2025). La inteligencia artificial en la guerra moderna. *Army University Press*.

- Barriga Carrera (2022), Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 15. Núm. 1 abril 2022.
- Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (25), pp. 8-23.
- Beaufre, A. (1963). *Introducción a la estrategia*. Editorial Rioplatense.
- Clausewitz, C. von. (1989). De la guerra (M. Howard & P. Paret, Eds. y Trads., p. 87). Princeton University Press. (Obra original publicada en 1832).
- Colmenares-Zapata, A. J. (2025). Nuevas amenazas a la seguridad humana en el siglo XXI: Aproximaciones multidimensionales y perspectivas latinoamericanas. *Revista Seguridad, Ciencia y Defensa*, 11 (11).
- Cornel Pillajo y Törn Narvaez, "La información como Instrumento de la guerra", Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 15. Núm. 1 abril 2022.
- Cuervo Ceballos (2018), Revista Científica General José María Córdova, vol.16 no.23 Bogotá July/Sep. 2018.
- Escobar-Jiménez, C. (2024). Estructuras internacionales del narcotráfico y factores socioeconómicos de la violencia en Ecuador. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (39), pp. 8-28.
- Ford, M. (2024). From innovation to participation: Connectivity and the conduct of contemporary warfare. *International Affairs*, 100 (4), pp. 1531-1549.
- Giannopoulos, G., et al. (2021). *The landscape of hybrid threats: A conceptual model*.
- Góngora Montejano, J. A. (2025). Elementos para la configuración de las amenazas híbridas y su proyección en la convergencia. *Revista de Estudios Políticos y Estratégicos*, 13 (2), pp. 164-185.
- Liddell Hart, B. H. (1967). *Strategy: The indirect approach* (pp. 5-10). Faber.
- Long, M. (2025). Shadows of power beneath the threshold: Where covert action, organized crime and irregular warfare converge. *Intelligence and National Security*, 40(1), pp. 87-113.
- Luvecce Ramírez, R. (2024). *Tecnologías de encriptación y el crimen organizado transnacional*. Universidad de Chile.
- Maquiavelo, N. (2003). *Del arte de la guerra*. Tecnos.
- Matiz, A., & Fernández, J. (2023). Inteligencia artificial en conflictos armados.
- Ministerio de Defensa Nacional del Ecuador. (2025). *Plan Nacional de Seguridad Integral 2025-2029*.

- Moncayo Gallegos, P. (2024). *Seguridad y defensa* (2.ª ed.). IAEN / ESPE.
- Observatorio Ecuatoriano de Crimen Organizado (OECO). (2025). *Informe de caracterización del crimen organizado en Ecuador 2025*. Fundación Panamericana para el Desarrollo
- Organización de las Naciones Unidas. (2004). *Convención contra la delincuencia organizada transnacional*.
- Peña-Galindo, A. (2026). Seguridad integral: Enfoques, dimensiones y actores. En *Seguridad integral y la resiliencia nacional: Preparación estratégica ante amenazas contemporáneas*.
- Rodríguez, E., Morales, R., Crescente, D., Cabello, M., & Paz, I. (2023). *La inteligencia artificial en la guerra híbrida como arma de desinformación*.
- Sisco Marcano, C., & Chacón Maldonado, O. (2004). Barry Buzan y la teoría de los complejos de seguridad. *Revista de Ciencia Política*, 25, pp. 125-146.
- Suleymanli, N., & Hajiyeve, T. (2024). The transformation of military strategy: The role of artificial intelligence in contemporary warfare and its implications for future conflicts. *Global Journal of Information Technology: Emerging Technologies*, 15 (1), pp. 16-22.
- Visceglie, G. (2022). Geopolítica del crimen organizado transnacional en las zonas fronterizas en Latinoamérica.
- Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (Eds.). (2021). *Hybrid warfare: Security and asymmetric conflict in international relations*. Bloomsbury Academic.



CAPÍTULO QUINTO

EL SALVADOR. COLEGIO DE ALTOS ESTUDIOS ESTRATÉGICOS

Influencia de las nuevas tecnologías en los escenarios de operaciones futuras

Francisco Yohalmo de Jesús Mejía Martínez

Resumen: Los avances tecnológicos han tenido una influencia determinante en las guerras más recientes, y, en aquellas que actualmente están en desarrollo. La Guerra del Peloponeso dejó muchas enseñanzas y quizás una de las más importantes es la comprensión sobre que el ser humano que desde hace más de dos milenios es exactamente el mismo que en el presente, y que lo único que va cambiando son los avances de la tecnología.

En la última década se ha visto la influencia de las nuevas tecnologías en los escenarios donde se están desarrollando guerras, específicamente, en la Guerra ruso-ucraniana que inició en el año 2022, y, la más reciente, la Guerra entre la alianza EE.UU.-Israel contra Irán. Algo de mucha importancia, es la conciencia de los multidominios que actualmente existen; es decir, los físicos (tierra, aire, mar y espacio) y los abstractos (ciber espacio).

El éxito o fracaso de las futuras guerras estará basado por diferentes aspectos, donde la tecnología es uno de sus principales; pero, también es vital las alianzas que se creen, asimismo, los líderes que estén tomando decisiones con rapidez y con determinación.

Palabras clave: Tecnología, Intereses Nacionales, Liderazgo, Geopolítica.

Acerca del autor: Cap. Nvo. DEMN Francisco Yohalmo de Jesús Mejía Martínez, se graduó de la Escuela Naval Arturo Prat de la República de Chile en el año 1997, Diplomado de Estado Mayor Naval en la Academia Naval de Guerra de la República de Chile en el 2015, Curso de Defensa Nacional y Postgrado en Seguridad y Desarrollo Nacional del Colegio de Altos Estudios Estratégicos 2022. Ha sido docente en el Instituto Especializado de Educación Superior para la Formación Diplomática IEESFORD y en la Universidad Evangélica de El Salvador.

Introducción

La Primera Guerra Mundial (transición a la guerra moderna) dejó como avances tecnológicos militares: el tanque, el avión de combate, el gas venenoso, los submarinos y las ametralladoras mejoradas; mientras que, la Segunda Guerra Mundial fueron: el radar (detección de aviones y barcos a larga distancia), la energía nuclear (bomba atómica), la computación como sistema, los primeros misiles balísticos (guiados y de crucero) y la aviación avanzada (bombarderos de largo alcance, aumento de la velocidad y capacidad bélica). Estos son unos ejemplos que permiten comprender los avances de la tecnología en la ciencias y artes militares.

En la Guerra del Golfo en 1991 se utilizó exitosamente la tecnología de las municiones de precisión (guiadas por laser), también generó grandes éxitos el avión F-117 Night Hawk con tecnología Stealth que no permitía ser detectado por los radares iraquíes. La guerra electrónica con los sistemas antimisiles (Patriot), fueron los avances tecnológicos militares más importantes para esta guerra, y que demostraron su efectividad contra Saddam Hussein.

Escribir sobre la influencia de las nuevas tecnologías en los escenarios de operaciones futuros es interesante, y a la vez, un desafío, principalmente por los eventos que han estado ocurriendo en los últimos años. Las nuevas tecnologías empleadas tanto en la Guerra ruso-ucraniana en el año 2022, y especialmente, en la Guerra EE.UU.-Israel contra Irán, han demostrado que la manera de hacer la guerra ha cambiado completamente.

En el período de los años de 2022 al 2026 los avances tecnológicos militares han sido sin precedente. En el año 2022, específicamente en la Guerra ruso-ucraniana, se observó una revolución tecnológica centrada en la guerra no

tripulada y la automatización, donde el uso táctico de los drones junto con el uso de la Inteligencia Artificial (IA, para reconocimiento) fueron vitales entre los antagonistas; mientras que, en la Guerra entre la alianza EE.UU.-Israel contra Irán se empleo fuertemente la IA para identificación, seguimiento y selección de objetivos de interés (TOI); asimismo, los misiles supersónicos y sistemas antidrones.

Entre 1970 y 1980, EE.UU. desarrolló su Doctrina basada en la batalla tierra-aire (AirLand Battle doctrine), que le permitió en esos años establecer una superioridad tecnológica en el balance de poder contra fuerzas soviéticas tras la guerra de Vietnam. Esta doctrina se basó en el despliegue de los cinco principales sistemas de armas: el tanque M1 Abrams, el vehículo de combate Bradley, el helicóptero AH-64 Apache, el helicóptero UH-60 Black Hawk y el sistema de defensa aérea Patriot.

La tecnología está avanzando a una velocidad supersónica que está impactando en diferentes ambitos de acción, y, su influencia en las operaciones está claramente identificada. Un ejemplo son los roles que cumplen los Estados a través de sus armadas o marinas de guerra, que para tal caso, son dos sus tareas; primero, está el rol de Defensa Nacional; y en segundo lugar, el rol de Seguridad Marítima. De ellas identificamos y distinguimos las denominadas operaciones militares y las operaciones distintas de la guerra. En ambas operaciones la tecnología juego un rol importante, y la historia lo ha demostrado, y en su mayoría el éxito esta en los líderes que han estado a cago de las operaciones.

Los Estados persiguen intereses nacionales, siendo estos los que iluminan y guían la Defensa Nacional, definiéndola como, "Conjunto de recursos y actividades que en forma coordinada desarrolla el Estado permanentemente en todos los campos de acción, para hacer frente a una amenaza a la soberanía nacional y a la integridad del territorio" (Asamblea Legislativa, 2002, p. 2); asimismo, los objetivos nacionales encierran esa concepción para lo que fueron creadas las armadas, marinas de guerra o fuerzas navales; es decir, la defensa de la soberanía e integridad del territorio marítimo; además, deben contribuir a mantener el buen orden en la mar¹, la paz, la prosperidad y la

¹ El concepto de buen orden en la mar significa un mar seguro, limpio y sin amenazas.

seguridad internacional. Para estas tareas es necesario la tecnología, específicamente, sensores, sistemas de armas, y todo aquello que ayuden al monitoreo, vigilancia, y control.

Los intereses nacionales son, “los que el grupo encargado de tomar decisiones en el gobierno determina que son importantes para el mantenimiento de la nación.” (Nicholas, Pickett, & Spears, 1959). Son esas aspiraciones supremas que no pueden ser negociables; y que, según Kenneth Waltz, “Los Estados deben perseguir sus intereses nacionales, y el interés nacional supremo es el aumento de la posición de poder del Estado”. (Waltz, 2001, p. 37).

El buque de guerra, es el núcleo estratégico de una armada, es el elemento más gravitante que con su presencia coarta la libertad de acción del oponente, es el obstáculo más grande para atacar los objetivos en posesión del adversario, y el almirante Alfred Mahan lo calificó como la llave de la estrategia marítima; asimismo, este buque como principal componente del poder naval, mediante sus atributos tiene la capacidad de radiar tantos distintos mensajes, que sus espectadores no distinguen o no descifran la intención verdadera. “La presencia visible de buques de guerra...[es] una amenaza de fuerza naval y, consecuentemente, un caso de diplomacia de cañoneras” (Cable, 1971, p. 6). La tecnología ha hecho que los sistemas de un buque de guerra facilite las diferentes tareas y roles que debe cumplir.

Los avances tecnológicos son los que otorgan a los buques de guerra su flexibilidad política y operativa inherente al poder naval. “El elefante no es vulnerable al cocodrilo mientras no se acerque a la ribera acuática” (Cable, 1971, p. 25), así es, mientras un Estado foráneo no amenace, “la integridad territorial e independencia política...intereses fundamentales de un Estado” (Hill, 1990, p. 13), entonces, todo será paz y cooperación. Este buque de guerra con personal altamente adiestrado y con la tecnología necesaria se convierte en una máquina imparable para alcanzar los objetivos nacionales.

Sumado a lo anterior, están los diferentes dominios en los cuales se desarrollan los actuales escenarios. Pero como bien es sabido, la tecnología esta al alcance de todas las Partes, y el dilema será en que lado esta el actor que mas simpatizamos.

Escribir sobre la influencia de las nuevas tecnologías en los escenarios de operaciones futuros es interesante, y a la vez, un desafío, principalmente por los eventos que han estado ocurriendo en los últimos años. Las nuevas tecnologías empleadas tanto en la Guerra ruso-ucraniana en el año 2022, y especialmente, en la Guerra EE.UU.-Israel contra Irán, han demostrado que la manera de hacer la guerra ha cambiado completamente.

Actualmente, es importante mencionar el equilibrio que debe existir entre el factor humano (su razonamiento) y la tecnología. Esto quiere decir que ninguno es más importante que el otro; sino, que lo que debe ocurrir es un balance. El profesor Milan Vego lo estableció en su famosa obra *Joint Operational Warfare*, en la cual argumentó que “en una guerra entre dos oponentes similares, la victoria será de los que piensan mejor, accionan más rápidamente y con mayor determinación. Esto no anula la necesidad de armas más avanzadas y equipo. Tampoco se puede insistir que el pensamiento superior es mucho más importante que la tecnología: el equilibrio es la clave”. (Vego, 2007, p. I-11). El tomar decisiones con determinación y rapidez, es de mucha importancia en la guerra para aprovechar las oportunidades que se presenten.

“La guerra de Vietnam demuestra que la superioridad tecnológica no conduce necesariamente al éxito operativo o estratégico.” (Till, 2009, p. 134), Lo mencionado por Geoffrey Till esta en la misma línea de pensamiento de Milan Vego y otros académicos. Es un equilibrio que debe existir; es decir, no es el más fuerte el que tendrá ese grado de victoria; sino, el que piense mejor, tome decisiones más rápido, actúe con determinación, y desde luego, logre ese equilibrio entre la tecnología y el razonamiento de sus planificadores y decisores.

Las operaciones distintas de la guerra, específicamente, las operaciones de interdicción marítima, que combaten los actualmente denominados Crímenes Azules (Blue Crime), como el tráfico de sustancias psicotrópicas y estupefacientes, trata de personas, tráfico de armas, y otros, están siendo afectadas; dado que, las estructuras dedicadas al narcotráfico y conexas tiene el capital económico en abundancia que les permite adquirir la última tecnología, y hasta cierto punto, son más eficaces que las autoridades que los combaten. Esto es una evidencia real de la influencia de la tecnología sobre las operaciones.

Hay evidencia que en el presente, el narcotráfico ya esta empleando semisumergibles no tripulados, lo que hace que su identificación y neutralización sean

cada día más difícil. También, estas estructuras están usando drones para detectar a las autoridades que se encuentran en patrulla; asimismo, ya poseen medios de comunicación cifrados, similares o mejores que los que poseen las instituciones de los Estados.

Entonces, la influencia de las nuevas tecnologías en los escenarios de operaciones futuros es un tema importante de analizar para ir tomando conciencia sobre los eventos que actualmente están en desarrollo o aquellos que se encuentran en su génesis.

Operaciones Multidominio y su impacto con la tecnología

El Ejército de EE.UU. define las operaciones multidominio como aquellas donde “la convergencia es la integración rápida y continua de capacidades en todos los dominios, el espectro electromagnético y el entorno de la información, que optimiza los efectos para superar al enemigo mediante la sinergia entre dominios y múltiples formas de ataque, todo ello facilitado por el mando de misión y una iniciativa disciplinada” (US Army War College, 2020, p. 45). Esto busca sincronizar capacidades en tierra, mar, aire, espacio y ciberespacio. Es de suma importancia profundizar en este tipo de operaciones para conocer aquella tecnología que se encuentra oculta, y así, prepararse a las nuevas formas de hacer la guerra.

Las capacidades kinéticas y no kinéticas son importantes en el escenario actual; dado que, no es únicamente con la fuerza física que puede ganarse la guerra; sino también, con otras capacidades necesarias como: los ciberataques a redes e instalaciones críticas y las operaciones de información. Esto también es parte de las operaciones multidominio que las fuerzas armadas desarrollan en el presente, y que lo estamos observando en los conflictos que se encuentran en desarrollo.

Está demostrado que la guerra ha cambiado por las diferentes dimensiones que existen, y que cada día hace más complejo los escenarios donde operan las fuerzas militares. En el año 2020 ya era un tema de discusión importante en diferentes colegios de guerra, donde se mencionó que “Estados Unidos se enfrentaba a adversarios en los dominios físicos del aire, la tierra, el mar y el

espacio, así como en los dominios abstractos del ciberespacio, el espectro electromagnético, el entorno de la información y la dimensión cognitiva." (US Army War College, 2020, p. 17). Esto ha hecho que el entrenamiento, la organización y el equipo sea cada día mas decisivo en el campo de batalla. El neoralista norteamericano Kenneth Waltz ya mencionó en su libro *The Man, State and War* que no hay perdedores; sino, que solo hay grados de derrota, y que el enemigo solo esperará la oportunidad para decapitar a su oponente.

La mejora continua en la Tecnología de la Información (IT/ sistemas informáticos) reducirá "la necesidad de que un humano en la cabina de un avión de ataque programe (o re programe) el arma después del despegue y antes de su entrega" (Till, 2009, p. 127). Esto no quiere decir que la tecnología es todo; sino, que simplemente facilita el desarrollo de las operaciones. La tecnología en general ha evolucionado conforme a las diferentes guerras registradas en la historia, y lo que debe entenderse es que el ser humano sigue siendo el mismo; es decir, ese individuo lleno de pasión, temores, ambiciones, odio, envidia, y tormentas interiores. Y lo interesante de analizar y debatir es, que, si ese individuo es capaz de controlar sus emociones y pasiones, entonces, podrá hacer un empleo eficiente de la tecnología a su disposición, para generar las ventajas necesarias hacia la victoria frente a su oponente.

El académico inglés Geoffrey Till argumenta en su obra *SEAPOW* un relato interesante que permite comprender como ha evolución la tecnología en las operaciones:

"En la Primera Guerra Mundial, el secreto del éxito radicaba en la coordinación eficaz de su artillería pesada. El almirante británico Madden lo explicó así en 1920: la concentración del fuego en un objetivo tras otro es el factor crucial en una batalla naval. En tiempos de Nelson, se trataba de controlar el fuego, posicionando varios barcos contra uno... Ahora, la artillería de la flota debía considerarse como un todo y, a menudo, ser dirigida desde el buque insignia hacia objetivos invisibles para el barco que disparaba. Para que este sistema de sistemas (¡por acuñar una frase!) funcionara correctamente, el comandante necesitaba información precisa sobre la posición exacta del enemigo durante la batalla (Till, 2009, p. 132)".

Por lo anterior, es que se afirma que la forma o manera de hacer la guerra ha cambiado, y es un mundo donde la tecnología ha evolucionado a pasos agigantados. Y por eso, la victoria relativa será para aquellos que tomen decisiones coherentes, de manera rápida, con determinación, y haciendo uso de las nuevas tecnologías. “Muchos argumentarían que las plataformas (portaviones, destructores, fragatas) serán cada vez menos el factor determinante a la hora de definir las características principales de las operaciones marítimas (terrestres y aéreas). En cambio, la atención debería centrarse en los sistemas, las armas y los sensores” (Till, 2009, p. 127). Para muchos la tecnología es todo; pero, el presente ha demostrado que no basta con tener eso; sino, que es una combinación de factores que permitirán la victoria, entre ellos, las alianzas correctas, visibles o percibidas.

Un ejemplo tomado como la génesis del término de las alianzas lo encontramos en la Guerra del Peloponeso, 432 a.C, donde se identifica constantemente las alianzas que los espartanos y los atenienses buscaban formar constantemente, considerando las fortalezas y debilidades de cada uno de ellos. Lo que estaban de moda en esa época era definirse como poder terrestre o como poder marítimo. Al final, luego que Atenas se convirtió en el imperio marítimo en ese momento, su arrogancia y abuso de los demás, hizo que sus aliados se alejaran de ellos y decidieran unirse en alianza con sus enemigos tradicionales (espartanos), y con los demás invasores como los persas. Entonces, las alianzas fueron y seguirán siendo un factor determinante a la hora de definir la victoria entre antagonistas.

La Estrategia de Defensa Nacional de 2018 de EE.UU. destaca los avances tecnológicos, como la inteligencia artificial, las armas hipersónicas y la robótica, junto con un aumento de actores no estatales que están cambiando la naturaleza de la guerra. Este punto fue respaldado y enfatizado por el general Mark Milley, entonces jefe del Estado Mayor del Ejército de los Estados Unidos, al afirmar que “los actores ambiguos, las intensas guerras de información y las tecnologías de vanguardia confundirán aún más la comprensión de la situación y desdibujarán las distinciones entre guerra y paz, combatiente y no combatiente, amigo y enemigo, e incluso, quizás, entre humanos y máquinas”.

Actores Geoestratégicos, sus operaciones multidominio y sus avances tecnológicos en el siglo XXI: China – EE.UU. – Rusia

Las superpotencias que aún mantienen su Estatura Estratégica en el s. XXI siguen siendo las mismas (China – EE.UU. – Rusia), y con base a la academia son definidos como actores geoestratégicos, que Brzezinski los definió como “los Estados con capacidad y voluntad nacional de ejercer poder o influencia más allá de sus fronteras para alterar el estado actual de las cuestiones geopolíticas...algunos Estados intentan alcanzar una posición de dominio regional o de importancia global...son empujados por motivaciones profundamente arraigadas y complejas” (Brzezinski, El gran tablero mundial. La Supremacía estadounidense y sus imperativos geoestratégicos., 1998, p. 49). Estas superpotencias son las que siempre están invirtiendo en la investigación y avances en nuevas tecnologías que le generen ventajas sobre sus competidores. La lucha por el poder jamás dejará de existir, y todo será argumentada basados en los intereses nacionales.

Es natural, estos actores tienen sus características que los distinguen como tales, por ejemplo, la importancia de Rusia es innegable, ya que su territorio “en el Ártico es 3.1 millones de km² -aproximadamente el tamaño de la India- lo que se traduce en 91% producción de su gas natural, 80% reserva de gas natural, 90% de sus reservas de hidrocarburo en alta mar.” (Brzezinski, 2012, p. 117). Y este actor en particular ha demostrado que sus intereses no serán menoscabados por otros Estados, y por lo tanto, empeña sus recursos para adquirir nuevas tecnologías, para fortalecer su poder en la región. Ahora bien, la gran competencia en tecnología es entre EE.UU. y China, y sus demostraciones son precisas y evidentes, aunque no de manera frontal.

Lo que el Orden Internacional espera es que ninguno de estos tres actores geoestratégicos emplee su arsenal nuclear, lo cual sería de mucho peligro para la humanidad.

EE.UU. ha demostrado en los últimos años su comportamiento tradicional de superpotencia; es decir, su realismo político. Acciones y decisiones racionales a su entender, y el mundo solo observando. Unos Estados a favor y otros disgustados; pero, como se ha mencionado es un comportamiento tradicional de las superpotencias. Algo que no puede negarse es, que EE.UU. sigue siendo la

superpotencia militar por excelencia; pero, eso no quiere decir que China y Rusia no pueda afectar sus intereses nacionales fuera de sus fronteras; dado que, es una competencia entre actores geoestratégicos.

La percepción del mundo actual bajo una estructura multipolar, ha venido acentuándose en los últimos años, por la aparición de actores emergentes en la era de la digitalización; evidentemente, existen resistencias para admitir la multiplicidad de agentes que coexisten en la definición de ese nuevo rumbo que el Orden Mundial está tomando, haciendo más complejas las interacciones en la Sociedad Internacional.

En tal sentido, hay que considerar que, en marzo del año 2023 China logró que Arabia Saudita y la República Islámica de Irán se acercaran y reanudaran sus relaciones diplomáticas, sobre esto, el profesor de la Universidad de Chicago, John Mearsheimer, durante el conversatorio *Why Israel is in deep trouble*, el 17 de mayo de 2024, en el Centro de Estudios Independientes (CIS) mencionó,

“Todos recordamos el día en que Estados Unidos y la Unión Soviética competían en el Medio Oriente. Bueno, lo que verán en el futuro no es solo Estados Unidos y Rusia, sino Estados Unidos, Rusia y China compitiendo en el Medio Oriente. Los chinos están construyendo una Armada de aguas azules para proyectar su poder...[ellos] dependen en gran medida del petróleo y, por lo tanto, están haciendo todo lo posible para tener buenas relaciones con Irán y con Arabia Saudita.” (Mearsheimer, 2024)”.

Es importante recordar que en 2024 la organización BRICS acrónimo de Brasil, Rusia, India, China y Sudáfrica anunciaron que habrían invitado a algunos Estados para adherirse al bloque de economías emergentes, caracterizada por su potencial para contrarrestar a la hegemonía económica occidental.

Actualmente, Irán ha dado muestras de robustez y liderazgo en el Medio Oriente, basado en las operaciones que ha llevado a cabo a partir de febrero de 2026. Siguiendo los términos establecidos en la academia, específicamente a la importancia del territorio iraní, se afirma que este Estado es un pivote geopolítico, que se define como aquellos,

“Estados cuya importancia se deriva no de su poder y de sus motivaciones sino más bien de su situación geográfica sensible y de las conse-

cuencias que provoca en el comportamiento de los jugadores geoestratégicos...los pivotes geopolíticos están determinados por su geografía, pueden definir las condiciones de acceso de un jugador significativo a áreas importantes o el de negarle ciertos recursos...un pivote geopolítico puede actuar como un escudo defensivo para un Estado vital o incluso para una región (Brzezinski, El gran tablero mundial. La Supremacía estadounidense y sus imperativos geoestratégicos., 1998, p. 49)".

Lo anterior, muestra claramente una de las razones o motivos que ocasionaron la Guerra entre EE.UU. e Israel contra Irán; es decir, la importancia estratégica de la posición geográfica del territorio iraní es lo que los actores geoestratégicos requieren. Unos de ellos deciden tomarlo mediante el hard power y otros con el soft power.

"La geografía siempre ha jugado un papel importante, por ejemplo: en el año 456 a.C. dos aliados de los espartanos, Corinto y Mégara, tuvieron una guerra por la frontera entre ellos. Mégara solicitó ayuda a Esparta para resolver esta crisis en contra de Corinto, pero los espartanos tomaron la decisión de no involucrarse; ante esto, Mégara pidió ayuda a Atenas, y estos, valorando la ventaja estratégica que les daría tener el territorio de Mégara para su seguridad y desarrollo, aceptó tomarlo como aliado. Parece ser que, en ese momento Atenas decidió minimizar los riesgos y maximizar los beneficios a favor de sus intereses nacionales, una acción que no dista en lo absoluto de la realidad. Ya bien lo decía Hans Morgenthau: los Estados no tienen alma. Sin embargo, son los Estados quienes deben tomar decisiones racionales, coherentes y sin pasiones, buscando siempre el bienestar supremo de su pueblo. (Mejía, 2024, p. 26)".

La historia es ciclica, y algunas veces será muy parecida a la realidad. Algunas investigaciones han hecho dejar ver que existe la posibilidad que un actor geoestratégico este atrás apoyando a Irán, principalmente, porque reconoce la importancia del territorio iraní y la cantidad de recursos naturales a los cuales tiene o puede tener acceso, y por lo tanto, es una asunto de interés nacional. Obviamente, ese acceso a sus recursos naturales es a cambio de asistencia en tecnología necesaria para enfrentar y resistir esa guerra. "No tenemos aliados eternos ni enemigos perpetuos, son nuestros intereses que son eternos y perpetuos, y es nuestro deber seguirlos" (Palmerston, 1848). El estadista británico

tenía razón al proclamar esta célebre frase, que únicamente expresa el realismo político de la época, y que continúa vigente en el presente.

La realidad muestra la importancia de las alianzas, que a través de ellas se da la cooperación y asistencia con adiestramiento, y sobre todo, con tecnología. Algo que los Estados y principalmente los actores geoestratégicos no deben olvidar es lo mencionado por Carl von Clausewitz, “El valor de juicio más trascendental que el político y un comandante tienen que hacer, es saber el tipo de guerra en la que se están embarcando...esta es la primera de todas las cuestiones estratégicas y que más debe ser comprendida”. (Howard & Paret, 1989, pp. 88,89)

Factores que determinaron el grado de derrota relativa entre la alianza de EE.UU. e Israel contra Irán: ¿Tecnología, liderazgo, estrategia?

El politólogo estadounidense Eliot Cohen y el historiador británico John Gooch han afirmado que los fracasos militares se encuentran en tres categorías básicas, “no aprender del pasado, no anticipar lo que el futuro puede traer, y no adaptarse a las circunstancias inmediatas en el campo de batalla” (Parshall & Tully, 2007, p. 402). Reflexiones importantes que dejan lecciones para analizar en el ambiente operacional del presente.

Lo ocurrido a partir del 28 de febrero de 2026 en el Medio Oriente es un claro ejemplo de cómo la tecnología es capaz de cambiar los resultados de una guerra. Jamás puede subestimarse al adversario por muy débil que parezca. La tecnología, el liderazgo, la rapidez y determinación en la toma de decisiones otorga una ventaja para aquel actor que se anticipa a los eventos.

En la Guerra de EE.UU. e Israel contra Irán, el grado de victoria relativa no se ha observado para el más fuerte; sino, para aquel que actuó mas rápido y con determinación, obviamente el empleo de la tecnología fue vital. Till ha mencionado que

“la tecnología hace que este sistema de mando, sensores y sistemas de ataque sea mucho más eficaz operativamente. El mando será más rápido y preciso. Los tiempos de reacción entre la identificación de un obje-

tivo y el lanzamiento de un ataque se reducirán de días (como en el caso de los ataques con misiles de crucero en 1991) a horas, e incluso minutos (o segundos). Esta reducción de tiempo se deberá en parte al procesamiento de datos más rápido gracias a la mayor capacidad de procesamiento informático y, en parte, a la aparición de medios de ataque con mejor tecnología (como los misiles supersónicos) (Till, 2009, p. 130)".

Pensar mejor, más rápido y con determinación es clave. La dimensión territorial de Israel (470 km por 135 kms) ha hecho más fácil el ataque para Irán. Las plataformas móviles de los misiles Fattah² combinado con los denominados enjambres de drones y el uso de misiles crucero y de otros tipo de armamento ha sido la estrategia de Irán para neutralizar en cierto grado el sistema de defensa aéreo israelí (Iron Dome/Domo de hierro, Arrow 3, David Sling); además, de la ventaja geográfica del territorio iraní, respecto a su dimensión (7400% más grande que Israel, o sea, Israel es 75 veces mas pequeño que Irán), que ha ocasionado que sea más difícil para Israel atacar las distintas bases estratégicas de misiles desplegados iraníes, sumado al constante movimiento de dichas plataformas.

El sistema de guiado que lleva instalado los misiles iraníes, permite ir cambiando constantemente su trayectoria, lo que confunde el sistema de defensa aéreo israelí. También, la saturación que sufrió este sistema otorgó un posicionamiento sólido de Irán para resistir. Todo esto ha permitido percibir que el sistema de defensa aérea israelí no está diseñado para contra atacar la estrategia iraní basada en la saturación de los misiles Fattah.

Este caso de estudio ha permitido percibir que la influencia de las nuevas tecnologías en los escenarios de operaciones futuros es determinante; pero, no

² Estos misiles hipersónicos tienen un alcance operacional promedio de 1,400 a 1,500 kilómetros, con velocidad máxima en promedio de entre 15,000 a 18,500 KPH; es decir, con un Mach entre 13 a 15 (Mach 1 equivale a 1,234.7 KPH o 767.269 MPH). Su sistema de propulsión SCRAM (combustión supersónica) hace que cuando el misil alcanza la atmósfera recoja oxígeno mientras viaja y adquiere la capacidad de acelerar, lo que aumenta más cuando esta a una distancia de 100 kilómetros del objetivo. Tiene 15.3 metros de largo y un peso de lanzamiento de alrededor de 12 toneladas; asimismo, su sistema de navegación satelital le permite una precisión entre 10 a 25 metros. Su plataforma móvil permite rápidos despliegues para su constante reubicaciones. Su capacidad de carga es de 200 a 500 kilogramos.

debe subestimarse la creatividad de los planificadores y la determinación para actuar.

Existe suficiente evidencia sobre lo vital que se convirtió el liderazgo en esta guerra. Para unos el liderazgo fue su fortaleza; mientras que, para otros fue un punto crítico que debilitó su centro de gravedad político-estratégico. Por un lado, sus líderes decidieron mantenerse firmes en sus pronunciamientos y no ceder; pero, otros decidieron de manera racional y realista no invadir el territorio adversario. Lo que no puede negarse es la importancia de la cohesión del liderazgo en tiempo de crisis.

Aquí toma sentido lo escrito por el Almirante William McRaven, de la Marina de Estados Unidos, mencionado en *The Wisdom of the Bullfrog* que:

“Siempre hay ejemplos de personas exitosas que carecen de escrúpulos, que no tienen brújula moral, pero que han ganado miles de millones de dólares y han llevado sus industrias a nuevas alturas. Pero la mayoría de las veces, es falta de integridad, hacer lo malo en lugar de lo correcto...Si violas tu juramento, tu código de conducta, la decencia básica con la que debes vivir tu vida y dirigir tu negocio, entonces eventualmente perderás el respeto de los hombres y mujeres a los que sirves, y lo contrario se convierte en tu destino...A menudo escucho, que es difícil saber qué es lo correcto. ¡No, no lo es! Siempre sabes lo que es correcto, pero a veces es muy difícil hacerlo. Es difícil porque es posible que tengas que admitir el fracaso. Es difícil porque la decisión correcta puede afectar a tus amigos y colegas. Es difícil porque es posible que no te beneficies personalmente de hacer lo correcto. Sí, es difícil. Eso se llama liderazgo. (2023, p. 9)”.

Tomar decisiones esquizofrénicas no es de un líder, y este código de conducta que menciona McRaven es algo que no todas las personas comprenden; pero, ese código de conducta sí hará la diferencia en la toma de decisiones durante el desarrollo de una guerra.

La destrucción de las bases norteamericanas en los países aliados en la región del Medio Oriente, hizo que EE.UU. no tuviese la capacidad de apoyo logístico necesario para continuar con el esfuerzo bélico; asimismo, esas mismas bases en esos países tenían la posición estratégica necesaria para atacar

a Irán y proteger a su aliado Israel; pero, sin esas bases EE.UU. careció de esa capacidad.

Fuchida Mitsuo, capitán de fragata y piloto de la Armada Imperial Japonesa, y uno de los planificadores del ataque a Pearl Harbor el 7 de diciembre de 1941, fue el creador de la frase: la Enfermedad de la Victoria y se refería comúnmente para “designar la actitud mental casual y demasiado segura... La pérdida resultante de la nitidez operativa...notó que el síntoma principal de la enfermedad fue la arrogante manera de subestimar al enemigo, así como su suposición de que el enemigo sería tomado por sorpresa, y esto fue lo que llevaba a la catástrofe!” (Parshall & Tully, 2007, p. 400). Esto le ocurre a muchos, y la historia lo ha demostrado constantemente. La Enfermedad de la Victoria confunde a los conductores políticos.

Es importante recordar que, durante la Guerra del Golfo en 1991, “los estadounidenses esperaban lograr una victoria rápida con armas de alta tecnología” (Gordon & Trainor, 1995, p. 163), y para ese caso, así fue, a pesar de los constantes errores de la inteligencia que tuvieron inicialmente los norteamericanos respecto a la cantidad de soldados iraquíes, los misiles y otros armamentos que los Saddam Hussein había adquirido en el mercado negro. La tecnología de esa época le permitió a EE.UU. cumplir en gran medida los objetivos que se habían establecido.

Los constates debates académicos como la literatura especializada han mostrado la efectividad, dificultades y el costo-beneficio del empleo de los portaviones en las operaciones actuales, y la cuestión fundamental, sin embargo, es que “el costo de realizar ciertas funciones debe compararse con el costo de no realizarlas o con el de otras alternativas. Por ejemplo, algunos han defendido un uso más extenso de misiles lanzados desde el mar o de artillería naval de largo alcance como alternativa a los costosos portaaviones” (Till, 2009, p. 126). Luego de la capacidad material demostrada por Irán en los constantes ataques que realizó con misiles supersónicos hacia Israel, y hacia las bases militares de EE.UU. en cercanías de Irán, es a partir del momento, que los planificadores y tomadores de decisión, específicamente, las superpotencias deberán valorar el empleo de los portaviones; primero, por los vulnerables que se vuelven frente a los enjambres de drones y misiles Fattah; y en segundo lugar, por el costo de los portaviones en comparación con otras opciones que han demostrado ser

efectivos; es decir, la tecnología ha permitido cumplir objetivos militares con un menor costo de producción.

Conclusiones

La llegada de la Inteligencia Artificial (IA) como representante de los avances tecnológicos, es la muestra que la imaginación y creatividad de los seres humanos no tiene límites.

Por décadas se ha mencionado que los grandes avances tecnológicos han encontrado su génesis en el ámbito militar, por mencionar un ejemplo, el internet. Y parece ser que, los diferentes conflictos y guerras son los laboratorios experimentales.

La Guerra del Golfo de 1991, todo el mundo pudo ver en sus casas en tiempo real lo que estaba ocurriendo al otro lado del mundo. Por eso, toma mucha importancia la frase que el ser humano de hace más de 2,500 años es el mismo; es decir, aquel individuo lleno de emociones, sentimientos, odio, envidia, amor y ambiciones por el poder. Y lo único que cambia son los avances tecnológicos.

En la última década, se han visto la influencia de las nuevas tecnologías en los escenarios donde se están desarrollando guerras, específicamente, en la Guerra ruso-ucraniana que inició en el año 2022, y, la más reciente, la Guerra entre la alianza EE.UU.-Israel contra Irán.

Conscientes de los diferentes dominios (físicos y abstractos) que existen, y en los cuales se están desarrollando o enfrentando los antagonicos, es que la influencia de la tecnología es determinante para el éxito en las operaciones presentes y futuras.

Como se ha mencionado en este ensayo, el éxito o fracaso en las futuras guerras estarán basado por diferentes aspectos, donde la tecnología es uno de sus elementos; pero, también ha quedado de manifiesto lo vital que son las alianzas y los líderes que estarán tomando decisiones racionales, rapidez y con determinación.

Referencias

- Brzezinski, Z. (1998). *El gran tablero mundial. La Supremacía estadounidense y sus imperativos geoestratégicos*. Barcelona: Paidós.
- Brzezinski, Z. (2012). *Strategic Vision. American and the crisis of Global Power*. New York: Basic Book.
- Cable, J. (1971). *Gunboat Diplomacy. Political applications of limited naval force*. London: Chatto and Windus Ltd.
- CODEM. (1999). *Texto de Estudio de Geopolítica para I año del CREM*. San Salvador: CODEM.
- College, U. A. (2020). The Need for Multi-Domain Operations. Strategic Studies Institute, US Army War College. Retrieved from <https://www.jstor.org/stable/resrep26552.8>
- Gordon, M., & Trainor, B. (1995). *The Generals' War*. New York: Back Bay Books.
- Hill, R. (1990). *Estrategia Marítima para Potencias Medianas*. Buenos Aires: Instituto de Publicaciones Navales.
- Howard, M., & Paret, P. (1989). *On War*. New Jersey: Princeton University Press.
- Kaplan, R. (2012). *The Revenge of Geography*. New York: RANDOM HOUSE.
- Mearsheimer, J. (2024, Mayo 17). Why Israel is in deep trouble. (T. Switzer, Interviewer) Center for Independent Studies (CIS).
- Mejía, F. Y. (2024). *Honor, Temor, e Interés. Motivos que condicionan el comportamiento de los Estados y de los seres humanos*. San Salvador: Sextante.
- Nicholas, J., Pickett, G., & Spears, W. (1959). The Joint and Combined Staff Officers Guide (Chapter 10). Washington: Army War Collage.
- Parshall, J., & Tully, A. (2007). *Shattered Sword*. Washington, D.C.: Potomac Books.
- Till, G. (2009). *SEAPOW. A Guide for the Twenty-First Century*. New York: ROUTLEDGE.
- US Army War College. (2020). *Enhancing Mission Command in Multi-Domain Operations: The Multi-Domain Operations Synchronization Process*. Strategic Studies Institute.



CAPITULO SEXTO

ESPAÑA, CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (CESEDEN)

El empleo militar de la Inteligencia Artificial

Carlos Javier Frías Sánchez

Resumen: La aparición de la Inteligencia Artificial (IA) es un factor crítico en el futuro de las operaciones militares. Las capacidades de la IA crecen a una velocidad inusitada y, con ellas, sus posibles aplicaciones militares. En el presente y en el futuro inmediato, la IA es una herramienta imprescindible para la automatización de numerosas actividades militares (desde el combate aéreo y antiaéreo a la optimización logística), pero también para el desarrollo de sistemas de armas autónomos y, especialmente, para la materialización del concepto de “campo de batalla transparente”.

Palabras clave: Inteligencia Artificial, vehículos autónomos, campo de batalla transparente, *kill chain*, *kill web*.

Acerca del autor: Carlos Javier Frías Sánchez, General de División del Ejército de Tierra de España. Jefe de la División de Desarrollo de la Fuerza del Estado Mayor Conjunto de la Defensa. Doctor en Paz y Seguridad Internacionales por el Instituto Universitario General Gutiérrez Mellado, Máster en Pensamiento Estratégico y Seguridad Global por la Universidad de Granada.

Introducción

La Inteligencia Artificial (IA) es un factor relativamente nuevo en el mundo militar. Sin embargo, a nadie escapa que ya hoy es un elemento decisivo que configura y condiciona la forma en la que los conflictos actuales se están desarrollando (aquellos que se producen entre Estados avanzados).

En realidad, la IA es una rama de la informática que busca desarrollar sistemas y máquinas capaces de *simular* capacidades humanas, como el aprendizaje, el razonamiento, la percepción, la creatividad y la planificación. Su objetivo es permitir que los computadores analicen datos, resuelvan problemas y, en una situación ideal, tomen decisiones acertadas de forma autónoma.

La definición presentada, subraya el carácter imitativo de la IA: *simula* unas capacidades humanas, que, en realidad no tiene. Esto es importante tenerlo en cuenta (como veremos más adelante), pero no disminuye las posibilidades que nos ofrece.

La Inteligencia Artificial (IA) puede clasificarse de muchas formas. A los efectos de este trabajo, no ahondaremos en las características técnicas que permiten el funcionamiento de los diferentes tipos de IA. En su lugar, emplearemos una clasificación que atiende a la filosofía que las anima y que, en consecuencia, nos debe permitir prever los resultados potenciales que ofrece. Así, dividiremos a la IA en tres grandes grupos:

- IA computacional: en entornos que responden a leyes físicas o matemáticas conocidas, gracias a la capacidad de cálculo de los ordenadores, esta IA es capaz de optimizar el resultado de sus acciones, pues puede calcular el resultado de todas las posibilidades de combinación de las variables que definen el entorno. Es la que se emplea en los programas de ajedrez o de *go*, por ejemplo.

- IA predictiva: este tipo de IA se orienta a detectar relaciones estadísticamente significativas entre los datos de entrada y los de salida. No es capaz de determinar el porqué de las relaciones que obtiene: simplemente presenta que existe una relación probabilística entre ellos. Los *Large Language Models* (LLM), como *ChatGPT*, *Perplexity*, *Claude* o *Grok* son los ejemplos más avanzados de este tipo de IA.
- IA cognitiva: la que *comprende* la relación entre los datos de entrada y de salida y es capaz de tomar decisiones por sí misma. Ésta se conoce en muchos casos como AGI o *Artificial General Intelligence* y sería una verdadera inteligencia, similar o, potencialmente, más avanzada que la humana.

En la práctica, estos modelos no son “puros”, sino que se basan cada uno en los anteriores. La IA cognitiva o “IA fuerte” es todavía una idea sin existencia real.

En el ámbito militar, cada uno de estos tipos de IA tienen múltiples utilidades.

La IA y sus usos militares

La IA nos permite, hoy, amplificar nuestras capacidades militares en aspectos tan distintos como la optimización logística, la guerra en el entorno ciber y las acciones en el dominio cognitivo. En el futuro, la aplicación de la IA se extenderá progresivamente a más campos de la actividad militar. Hipotéticamente, en el futuro la AGI podría llegar a planear y conducir al nivel más alto las operaciones militares, pero todavía no está en condiciones de hacerlo.

Como se ha citado, la Inteligencia Artificial computacional no es más que la optimización mediante medios informáticos de problemas que responden a un número finito de reglas fijas. Un ejemplo sencillo serían los juegos como el ajedrez o el *go*. En ambos casos, el número de jugadas posibles es enorme, pero, al final, es finito. De la misma forma, las piezas en ambos juegos obedecen a reglas fijas que no varían: en el ajedrez, cada pieza tiene una capacidad de movimiento determinada por las reglas del juego. Gracias a la potencia de cálculo de los sistemas informáticos, un ordenador es capaz de optimizar el juego, realizando un número tan grande como sea necesario de cálculo de jugadas para obtener un resultado deseado. De hecho, una de las primeras aplicaciones populares de este tipo de IA

fueron las máquinas de ajedrez y los programas que permiten a un ordenador emularlas. El *go*, un juego muy popular en Asia y más complejo que el ajedrez, comparte con éste que obedece a una serie de reglas fijas, por lo que pronto se consiguió que una máquina pudiese vencer al mejor maestro humano es este juego, como había ocurrido algún tiempo atrás en el ajedrez.

En las operaciones militares hay un número mayor de lo aparente de actividades que responden a este patrón: están sujetas a reglas conocidas que no pueden variar. Como ejemplo puede citarse el combate aéreo: las aeronaves se desplazan por un medio físico conocido - el aire - y tienen unas características técnicas conocidas que les dan una serie de capacidades que no pueden modificar (velocidad máxima, aceleración, maniobrabilidad, detectabilidad ante el radar...). Como consecuencia, es una actividad muy adecuada para el empleo de IA computacional. No obstante, no es la única. Otro ejemplo es el combate antiaéreo: conocemos el objetivo a defender, el terreno (que, en general, estará perfectamente cartografiado y digitalizado), las características de las aeronaves y las armas enemigas y las de los sensores y los sistemas de armas propios. Y todos ellos están sujetos a leyes físicas conocidas. De forma similar, es posible emplear esta IA en otros campos menos evidentes, pero que comparten las características citadas: existencia de leyes físicas que las gobiernan y un número limitado (por grande que pudiera ser) de variables. Es el caso de la EW y de gran parte de las actividades que se realizan en el ciberespacio, pero también de la Logística, donde se conocen los consumos, las existencias, las rutas de abastecimiento disponibles, los medios de transporte... Es decir, la IA computacional puede adquirir un papel muy relevante en multitud de actividades críticas en el campo militar, con la ventaja añadida de que, en esencia, solo depende de la capacidad de cálculo de los equipos informáticos. Como consecuencia, es de aplicación directa en las operaciones actuales.

En el caso de la IA computacional, existen gran cantidad de actividades militares que responden a las características que necesita esta IA: entorno que responde a leyes físicas y número de variables limitado (aunque pueda ser muy grande). Los casos de empleo más evidentes podrían ser los cálculos logísticos o la optimización del tráfico en una red viaria. Sin embargo, también es el caso

del combate aire-aire (las aeronaves se mueven en un entorno físico de leyes conocidas y sus características técnicas, también conocidas, hacen que su comportamiento pueda ser predecible), o de la defensa antiaérea (el terreno es conocido y está cartografiado y digitalizado, y los sistemas de defensa aérea, como los aviones, también tienen características técnicas conocidas). Igual ocurre en otros campos, como el ciberespacio o la gestión del espectro electromagnético.

La IA predictiva tiene un número creciente de aplicaciones. La más evidente es su empleo para el análisis de inteligencia: este tipo de IA es capaz de convertir en información útil una ingente cantidad de datos procedentes de fuentes diversas. Empresas como *Palantir* emplean este tipo de IA para gestionar los datos procedentes de miles de sensores y transformarlos en información, lo que no podría hacerse con métodos manuales. Esta función es crítica para el combate en el “campo de batalla transparente”, caracterizado por la disposición de una enorme cantidad de sensores que proporcionan una cantidad ingente de datos, cuyo proceso solo es posible gracias a la IA.

La IA predictiva se caracteriza porque el algoritmo intenta encontrar la respuesta al problema planteado a partir de datos estadísticos previamente cargados. Un ejemplo sencillo es el corrector de los teléfonos móviles: cuando estamos escribiendo un mensaje, todos podemos ver cómo el software nos va “sugiriendo” la palabra siguiente o corrigiendo nuestra escritura si detecta una incongruencia con la palabra que espera o una grafía distinta de la que conoce. Estos sistemas “aprenden” de nuestro comportamiento y personalizan sus sugerencias en función de la experiencia previa adquirida del tipo de mensajes que solemos escribir. La IA predictiva trata de encontrar la cadena de caracteres futura en función de lo que tiene en sus bases de datos y de la experiencia adquirida en su uso. Es interesante recordar que los *Large Language Models* (LLM) operan de esta forma: mediante el “prompt” le damos un “contexto” que orienta al software sobre el tipo de bases de datos que debe consultar, el objeto de la consulta y el tipo de respuesta esperada, y eso permite al software generar la cadena de caracteres que forma su respuesta. Es importante subrayar que el LLM no comprende ni la pregunta ni la respuesta: somos nosotros, los seres humanos, los que damos significado a un determinado resultado estadístico. Esta forma de funcionar nos permite comprender la

importancia de las bases de datos: sin ellas, el mejor algoritmo de IA existente sería incapaz de proporcionar respuestas atinadas. Igualmente, esto resalta la necesidad de “entrenar” a la IA: solo realizando múltiples repeticiones, la IA es capaz de determinar la prioridad estadística de una determinada palabra (que, para nosotros, representa un “concepto”). Los LLM “generalistas” (los citados *ChatGPT*, *Perplexity*, *Claude*...) aprenden continuamente gracias a la interacción permanente con sus usuarios a través de Internet. De esta forma, refinan constantemente sus respuestas y amplían sus bases de datos.

Por su propio funcionamiento, la IA predictiva es muy adecuada para obtener patrones estadísticos significativos a partir de datos aparentemente inconexos. Así, una IA de este tipo es capaz de predecir enfermedades a partir de colecciones de datos que, para los humanos, tendrían muy poca relevancia (interpretando mínimas variaciones en una radiografía, por ejemplo, que, si se repiten en el caso de algunas enfermedades, dan lugar a un “patrón” de resultados estadísticamente significativos). Siguiendo con el ejemplo, la IA predictiva es incapaz de comprender las razones por las cuales esa marca en la radiografía implica una cierta probabilidad de tener una enfermedad determinada, pero sí es capaz de establecer que, estadísticamente, hay una relación. Nuevamente, esto subraya la importancia del “entrenamiento”: cuantas más radiografías analice la IA, más fiables serán los “patrones” que detecte.

En este sentido, es importante destacar que los seres humanos aplicamos regularmente ese tipo de inteligencia: por ejemplo, cuando caminamos y llegamos a una escalera somos capaces de identificar los escalones porque los empleamos regularmente, aunque, cuando éramos pequeños, era fácil que tropezásemos y cayésemos. Nuestra inteligencia no estaba “entrenada”). Nuestra vida diaria está llena de acciones que se basan en esa inteligencia predictiva, que nace de la experiencia.

La IA predictiva tiene importantísimas aplicaciones en el campo militar. Su capacidad de reconocer patrones le otorga una utilidad enorme en el campo de la información (en términos militares, de la “Inteligencia”). Como ejemplo, no hace muchos años, una de las principales fuentes de Inteligencia era la fotografía aérea o de satélite. Cuando un avión de reco-

nocimiento (o un satélite) proporcionaba una fotografía de un determinado lugar, era necesario “analizarla”: personal especialista en fotografía aérea, empleando aparatos espaciales (los estenógrafos) y lentes de aumento recorrían la imagen para tratar de detectar algún elemento de interés. Además de ello, debían identificar el lugar donde había sido tomada la foto, la hora del día, etc. Este análisis duraba un tiempo largo (varias horas por cada foto), dependía del concurso de personal especializado y escaso y, ademase estaba sujeto a que algún elemento presente en la imagen pasase desapercibido. En cambio, los sistemas de IA predictiva son capaces de analizar miles de fotos por segundo, identificar todos los elementos presentes y detectar “patrones” que pueden pasar desapercibidos para el analista que solo ha analizado unas pocas fotos de una serie determinada. Esta capacidad es crítica para la operación de sistemas de adquisición de objetivos, descritos luego como “kill chains” y “kill webs”.

Además de esa capacidad de análisis, la IA predictiva puede realizar otra función crítica en el campo de la Inteligencia: la “correlación” de datos. En efecto, es posible que un mismo objetivo sea detectado por diferentes sensores (por un avión de reconocimiento, por un satélite y por un radar terrestre, por ejemplo). Para el analista humano, esto implica que debe determinar si se trata de un solo objetivo o son tres diferentes. Esta labor, que no es sencilla, le resulta casi inmediata a una IA predictiva. Y, como consecuencia, esta IA es capaz de realizar la “fusión de datos”: recibir información procedente de múltiples sensores conectados y eliminar las duplicidades. Y, además, puede hacerlo de forma continua, por lo que puede proporcionar una imagen casi en “tiempo real” de la información obtenida por los sensores disponibles. Como las capacidades de los sistemas informáticos actuales son muy potentes, la IA predictiva puede recibir información de un número enorme de sensores. Es decir, si contamos con el número suficiente de sensores (aviones de reconocimiento, satélites, UAS, radares, sensores ópticos, teléfonos móviles, datos públicos de Internet...) un sistema de IA predictivo puede proporcionarnos una imagen muy actualizada de la situación de todos los elementos presentes en el campo de batalla.

En este punto, es interesante recordar que, durante la mayor parte de la Historia, para los contendientes, el campo de batalla era un lugar esen-

cialmente desconocido. De hecho, son comunes expresiones como la de “la niebla de la guerra” de Clausewitz o “el otro lado de la colina” de Wellington. El jefe militar conocía muy poco de la disposición y fuerzas de su enemigo, esencialmente porque disponía de muy pocos medios de obtención de información y porque la velocidad de transmisión de la información obtenida no superaba la del galope del caballo o el vuelo de la paloma mensajera. En realidad, los “sensores” disponibles eran apenas unas pocas unidades de Caballería o Infantería ligera, algún espía ocasional, y, más recientemente, un número limitado de medios aéreos, observatorios o equipos de EW... Como consecuencia de esta escasez, el jefe militar debía sopesar cuidadosamente dónde y cuándo emplearlos. Así, el campo de batalla era un espacio completamente oscuro en el que el jefe militar solo podía “iluminar” unos pocos lugares con los “sensores” de que disponía. Conforme la tecnología va mejorando, el jefe militar recibe más información, y el campo de batalla presenta menos zonas de oscuridad. Sin embargo, es en el conflicto de Ucrania, con el empleo de decenas de miles de UAS y centenares de miles de teléfonos móviles y otros sensores cuando la masa de datos disponible supera la capacidad humana de procesamiento. Y es en ese momento cuando la IA predictiva muestra su valor: solo la IA es capaz de procesar la ingente masa de datos procedentes de la cantidad inédita de sensores de que disponen hoy las FFAA de los Estados en conflicto.

Otra utilidad igualmente importante pero menos conocida es su empleo en vehículos autónomos. En realidad, la guía de vehículos autónomos es una aplicación de este tipo de IA: estos sistemas reconocen su entorno gracias a sistemas de IA predictiva, que les permite reconocer que determinadas imágenes (al final, conjuntos de píxeles recogidos por un sensor) representan obstáculos en el terreno que deben sortear o caminos que deben emplear. En efecto, los seres humanos basamos gran parte de nuestra movilidad en el reconocimiento de patrones: los conductores identifican las señales de tráfico, la calzada, las rayas de la carretera, los socavones... gracias a la experiencia acumulada. Pero acciones tan sencillas como caminar, subir una escalera u orientarse en una ciudad no son más que el empleo por el cerebro humano de patrones aprendidos. De la misma forma, la IA predictiva es capaz de controlar máquinas capaces de moverse por diferentes medios de

forma autónoma. La experiencia del Teatro de Operaciones ucraniano nos permite valorar la importancia militar de estos sistemas.

Un efecto añadido de la popularización de este tipo de IA es la "democratización" de la precisión: los sistemas de guiado apoyados en IA (aunque también en sensores tradicionales) han puesto a disposición de cualquier actor estratégico (estatal o no) armas de largo alcance y gran precisión, que, hasta hace bien poco, solo estaban al alcance de las Grandes Potencias.

Los LLM están empezando a utilizarse como medios de ayuda a la decisión, pero, en realidad, no son más que usos de la IA predictiva: el programa entiende que, en un contexto determinado (creado por el usuario al plantear el problema), detrás de una palabra determinada, la que tiene más posibilidades de aparecer es otra concreta (como hacen los correctores de los teléfonos móviles). Esto pone de relieve las muchas limitaciones de estos LLM y la necesidad de supervisar siempre sus resultados.

La IA predictiva es una evolución de la IA computacional y, en realidad, es muy difícil distinguir dónde termina una y empieza la otra: en la práctica, el software de ambas tiene muchas partes comunes, y muchas funciones de la IA predictiva se apoyan en IA computacional. En cualquier caso, si combinamos las posibilidades de la IA predictiva y la IA computacional, es posible tener una IA predictiva que fusione la información procedente de miles de sensores, obtenga una imagen de lo que aparece en el campo de batalla, lo compare con la información disponible de la forma de operar de nuestro enemigo y determine (estadísticamente) qué está haciendo. Con la información de los medios enemigos presentes en el campo de batalla y de los vectores de fuego disponibles, una IA computacional podría optimizar las capacidades de fuego propias para batir el mayor número posible de los objetivos enemigos detectados, con la prioridad que determine la valoración de intenciones del enemigo (por ejemplo, si la IA predictiva entiende que el enemigo pretende hacer un paso de río, podría priorizar batir a las unidades de pontoneros). Esto, con algunas limitaciones, es ya una realidad en los campos de batalla de Ucrania, Gaza o Irán.

La IA predictiva tiene otras aplicaciones militares importantes. En el mundo presente (y, aún más, en el futuro), la posibilidad de influir directamente sobre

la opinión pública del adversario será una práctica habitual. En general, la forma más probable de acceder a esa opinión pública será a través de Internet, manipulando las redes sociales, los medios de comunicación, o, incluso, las bases de datos que alimentan las IA predictivas "generalistas". La IA predictiva es capaz de producir excelentes análisis de los puntos débiles y fuertes de una determinada audiencia, e, incluso de sugerir temas que creen las emociones buscadas en la audiencia objetivo. De la misma forma, es capaz de "inundar" las bases de datos que se desee con contenidos falseados, de forma que altere los resultados que ofrecen las IA generalistas a cuestiones que afecten a los intereses propios. Como en el caso anterior, esto no es futuro: es presente. Y será un fenómeno más habitual en el futuro.

La IA predictiva también es capaz de detectar todo lo que se conecta a Internet, buscar vulnerabilidades en el software de acceso o de operación de cualquier de ellos y "hackearlo" para producir los efectos que se deseen. Conforme aumente la cantidad de dispositivos conectados (el "Internet de las cosas") la posibilidad de causar daños físicos por medios cibernéticos crecerá exponencialmente. Pero, de la misma forma, se mantendrá la dificultad de atribución de posibles ataques inherente a las acciones ciberespaciales. Y, como consecuencia, la frecuencia y el impacto destructivo de este tipo de acciones no hará más que incrementarse.

En cuanto a la IA cognitiva, ésta no existe... todavía. Pero es importante subrayar el término *todavía*. Los avances en la capacidad de los ordenadores (y aún más con la llegada de los ordenadores cuánticos) hacen previsible que ésta aparezca en un plazo de tiempo más o menos breve. Consecuentemente, su empleo en el campo de batalla es igualmente probable.

En teoría, esta IA cognitiva podría emplearse para dirigir las operaciones militares y no como un simple auxiliar para tareas concretas. Sin embargo, como hemos citado anteriormente, una IA necesita una base de datos. Y no una cualquiera: debe ser completa (contemplar todos los casos de un mismo fenómeno, o una amplia mayoría de ellos), representativa (debe representar fielmente la frecuencia de aparición de cualquier característica en el fenómeno que quiere representar), significativa (presentando aquellas características que sean relevantes para el fenómeno que trata)... La po-

sible utilización militar de una futura IA cognitiva nos lleva a preguntarnos ¿qué sabemos de la guerra? Pues, en realidad, poco.

Para ser fiables, estas bases de datos deben ser lo suficientemente grandes, representativas del fenómeno a tratar y que contemplen todos los aspectos de la cuestión. En el caso del fenómeno de la guerra, la página [The Correlates of War Project – The Correlates of War Project](#) recoge la base de datos más completa sobre conflictos militares. En esa recopilación han identificado poco más de 2.500 conflictos. No es un número pequeño, pero, de cara a la estadística, tampoco es excesivamente grande. El problema aparece cuando incluimos el dato de que estos 2.500 conflictos se expanden durante más de 10.000 años de historia, con las enormes variaciones tecnológicas implicadas (con un efecto muchas veces decisivo en el desarrollo de estos conflictos). Y, además, la información disponible es incompleta (de algunos de ellos, apenas sabemos poco más que su existencia) y poco fiable (“la historia la escriben los vencedores” ...). Es decir, no hay mucho material para “entrenar” una IA cognitiva. Sin embargo, estas mismas limitaciones son aplicables a los decisores humanos: tampoco disponemos de más información para aprender “el oficio de las Armas” de la que podemos entregar a una futura IA cognitiva. Es decir, no tenemos garantías de que un general humano vaya a hacerlo mejor que una IA. En realidad, una IA es capaz de recopilar una ingente cantidad de datos, mucho mayor que la que está alcance del ser humano individual. En consecuencia, dependiendo de su capacidad de comprensión, en principio tendría más capacidad que el humano promedio...

Un camino alternativo, pero prometedor, es la generación de “datos sintéticos”, es decir, crear simulaciones informáticas de conflictos cuyo desarrollo y resultados permitan entrenar a una futura IA cognitiva. Empleando esta técnica, es posible expandir la base de datos tanto como sea necesario. A cambio, las simulaciones informáticas solo emplean un conjunto limitado de parámetros (los que decide el diseñador de software), mientras que la experiencia histórica muestra que existen multitud de elementos muy difíciles de parametrizar: la moral, la preparación de las tropas, la calidad del mando, los actos individuales... Es decir, estas simulaciones siempre serán incompletas y los “datos sintéticos” obtenidos nunca podrán reemplazar a la experiencia real. Sin embargo, pueden ofrecer una mejora suficiente a la IA cognitiva como para

capacitarla para realizar esas funciones de planeamiento y conducción militar al más alto nivel.

Ya hoy, los conflictos de Ucrania, Gaza o Irán son ejemplos de empleo actual de la IA. En los tres casos, el espacio de batalla se configura como un espacio “transparente”, en el que operan miles de sensores de tipos varios (desde satélites civiles o militares hasta decenas de miles de UAV y cientos de miles de smartphones). Esta enorme cantidad de sensores genera un volumen de datos que solo la IA es capaz de transformar en información sobre la que se pueden tomar decisiones. El combate es hoy un intercambio de fuegos, en el que las fuerzas armadas contendientes se conforman como una cadena de fuegos (“kill chain”), cuyas etapas responden al acrónimo inglés “F2T2EA” (*Find, Fix, Track, Target, Engage, Assess*). La IA computacional y la predictiva son fundamentales en la ejecución de todas y cada una de estas etapas, como se describirá en el sucintamente a continuación.

“Kill chains” y “kill webs”

El campo de batalla actual es ya “transparente”: gracias a la enorme cantidad de sensores a disposición de los ejércitos, todo lo que se despliegue en el campo de batalla puede ser detectado y, debido al gran abaratamiento de los sistemas de guiado, todo lo que se detecte puede ser atacado con armas de precisión.

Las organizaciones militares disponen de estructuras específicas para acometer la destrucción de objetivos detectados. En términos occidentales, se denominan “kill chains”.

Una “kill chain” se articula en una serie de pasos, con unos medios militares determinados dedicados específicamente a ejecutar cada uno de ellos. En general, una de estas “kill chains” se organiza en seis pasos: Find (detectar), Fix (localizar), Track (seguir), Target (incluirlo en una lista de objetivos), Engage (atacarlo con un sistema de armas) y Assess (determinar el resultado del ataque).

Hasta los años 90, los medios disponibles para cada uno de estos pasos eran limitados:

- Find: como hemos citado, los medios de obtención disponibles eran limitados. Apenas se disponía de un puñado de aviones de reconocimiento fotográfico, algunas unidades de reconocimiento terrestre, observadores avanzados de artillería, equipos de EW y, las Grandes Potencias, satélites.
- Fix: como también relatamos, la determinación de las coordenadas de los objetivos era un proceso lento y trabajoso. En el caso de las fotografías aéreas, era necesario que el avión regresase a su base, se revelase la película (normalmente de nitrocelulosa), se analizase cada una de las fotografías obtenidas y se determinase el lugar donde habían sido tomadas... En el caso de las unidades terrestres (de reconocimiento u observadores), su acción estaba limitada a la zona más inmediata a la línea de contacto entre los contendientes, por lo que la localización era más rápida, pero limitada a esta zona. En el caso de los satélites, era necesario esperar a que el satélite pasase por la zona de interés y la imagen obtenida requería un análisis similar a la fotografía aérea.
- Track: cuando se detectaba un objetivo en movimiento, los medios para mantener actualizada su posición eran, esencialmente, los mismos que para los pasos anteriores: escasos y lentos. En consecuencia, era muy sencillo para un objetivo móvil escapar a la acción de los vectores de fuego, simplemente cambiando de posición con mayor frecuencia que la duración de la "kill chain".
- Target: una vez se detectaba una cantidad suficiente de objetivos (o de forma periódica), era necesario decidir cuáles de ellos era posible batir con los vectores de fuego disponibles y con qué prioridad. La creación de "carpetas de objetivos" era un proceso largo, en el que se valoraba desde el tipo de armas necesario para conseguir los efectos deseados hasta las probabilidades de "daños colaterales" o su adecuación al Derecho de los Conflictos Armados. Adicionalmente, cada mando militar implicado intentaba que los objetivos ligados al cumplimiento de su misión particular recibiesen una mayor prioridad, lo que llevaba a discusiones y "negociaciones" para llegar a una lista consensuada. Por todo esto, la confección de una lista priorizada de objetivos era un proceso igualmente complejo y tedioso.
- Engage: obtenida la lista, los sistemas de armas recibían los objetivos que debían batir, el momento de hacerlo y los efectos a lograr. Con estos datos

iniciaban su propio planeamiento para estar en condiciones de cumplir con la tarea asignada.

- Assess: realizado el ataque, era necesario comprobar si se habían alcanzado los objetivos deseados. Para ello, nuevamente, los medios disponibles eran los escasos sensores empleados para las fases de Find y Track...

Durante los largos años de la Guerra Fría, la OTAN desarrolló una importante experiencia en este proceso. Y, aun así, el número de objetivos que podía generar un Cuartel General de OTAN se reducía a doscientos o trescientos, de los que poseía batir solo una parte. El tiempo para completar esta "kill chain" era de unas 72 h. Es decir, desde que se detectaba un objetivo hasta que se atacaba y se comprobaban los efectos del ataque, transcurría un periodo de tres días. Obviamente, los objetivos móviles presentaban enormes problemas (como mostró la fallida "Scud Hunt" de la Guerra del Golfo de 1991). Sin embargo, con los medios de la época, poco más se podía hacer...

En el periodo de tiempo transcurrido entre el final de la Guerra Fría en 1991 y el inicio de la Guerra de Ucrania en 2022, se produce el mayor avance tecnológico de la historia humana. Y la ejecución de esta "kill chain" no podía ser ajena a este avance.

El primer cambio importante es la multiplicación de los sensores. A los sensores militares tradicionales reseñados, se van uniando progresivamente satélites civiles de observación, UAS militares, teléfonos móviles... Al poco tiempo de la invasión de Ucrania, las fuerzas armadas de este país incorporan masivamente los teléfonos móviles, los UAS militares y multitud de pequeños y baratos UAS civiles a su arsenal de sensores, que, de esta forma, pasa de contar unas pocas docenas de sensores a componerse de varias decenas de miles de ellos (de millones, si contamos a los teléfonos móviles en manos de civiles ucranianos). Por primera vez en la historia, la cantidad de información que generan los sensores supera con creces la capacidad de los mandos militares de procesarla. Como consecuencia, los ucranianos descentralizan el control su "kill chain": en lugar de un sistema centralizado, cada Brigada ucraniana crea su propia "kill chain" con los medios que tiene a su alcance. Pero la duración de esta "kill chain" se comprime enormemente, por buenas razones:

- Find: disponiendo de miles de UAS, se mantiene una observación casi constante del sector defensivo de cada Brigada. Estos UAS disponen de cámaras que envían información en tiempo real a su estación de control, es decir, no hay “tiempo de revelado” ni hay “tiempo de análisis”.
- Fix: gracias a la introducción del GPS, la información obtenida viene georeferenciada. No hay necesidad de hacerlo manualmente.
- Track: los UAS pueden permanecer un tiempo relativamente prolongado sobre una zona, lo que permite mantener permanentemente el seguimiento de los objetivos detectados.
- Target: al descentralizar la autoridad para atacar objetivos, las decisiones son más sencillas y más rápidas. Adicionalmente, la precisión de las nuevas armas hace innecesaria la valoración de “daños colaterales”, lo que supone otro ahorro de tiempo.
- Engage: muchos de estos UAS están armados y son fungibles (“municiones merodeadoras”) por lo que la decisión de destruir un objetivo es simultánea con atacarlo.
- Assess: los sensores del UAS mantienen el seguimiento sobre el objetivo hasta el último momento, lo que permite tener una idea bastante aproximada (e inmediata) del efecto conseguido.

En conjunto, las “kill chain” ucranianas pasan de necesitar 72 h a pocos minutos. A cambio, su profundidad es muy limitada: los pequeños UAS en los que se basan sus “kill chains” tienen una autonomía muy limitada, por lo que solo operan a pocos kilómetros en la profundidad del dispositivo ruso.

Poco después del inicio del conflicto, Ucrania recibe una ayuda importante. La empresa *Palantir* ofrece sus servicios a las Fuerzas Armadas de Ucrania (FAU). Su producto estrella es *Gotham*, un software de fusión de datos basado en IA predictiva, con la capacidad de integrar la información procedente de un número casi ilimitado de sensores. Esto permite a las FAU integrar la información que tenía diseminada por sus Brigadas: las pequeñas “kill chains” ucranianas se van integrando en una mucho mayor, pero con la misma agilidad.

Paralelamente, las FAU desarrollan nuevos modelos de UAS, dotados de armas más potentes y pesadas y con capacidad de penetrar mucho más en la retaguardia enemiga. Para gestionar esta “kill chain”, las FAU emplean tecno-

logía de *Palantir*, que es capaz de generar automáticamente listas de objetivos y asignarlos directamente a los vectores de fuego disponibles.

La introducción del software de *Palantir* hace que la “kill chain” se convierta en una “kill web”: cualquier vector puede hacer fuego con datos procedentes de cualquier sensor. Esta forma de trabajar da una enorme flexibilidad al sistema de fuegos ucraniano... Y habría sido imposible sin la participación de la IA (es imposible para los seres humanos procesar en tiempo útil masas de datos que se miden en Petabytes) y, de forma complementaria, sin la capacidad de intercambiar información a través de Internet, gracias a los satélites de StarLink.

La “kill web” generada es, en la práctica, un enorme sistema integrado, que puede ser tan autónomo como se desee. En realidad, el sistema podría operar con mínima intervención humana, y la poca actuación de seres humanos estaría centrada en las etapas más inocuas del proceso: el control de los UAS o dar la orden de fuego a sistemas de armas... Sobre objetivos decididos y asignados exclusivamente mediante IA. El sistema permite que las decisiones críticas se reserven a los seres humanos... Si así se decide. El problema es que la acción humana ralentiza la ejecución de la “kill web”, por lo que, si se enfrentan dos sistemas similares, aquel que no incluya decisiones humanas (“man in the loop”) podrá reaccionar de forma más rápida, lo que le daría una ventaja potencialmente decisiva. Esto supone un poderoso incentivo para dar más y más capacidad de decisión autónoma a la IA, lo que abre debates filosóficos y morales de enorme importancia.

Conclusiones

La IA no es el futuro en el campo militar: es el presente. Sin embargo, sí es posible asegurar que se convertirá progresivamente en una capacidad imprescindible. Ya hoy, la IA otorga una ventaja capital al combatiente que disponga de ella, pues le permite – con el concurso de sensores y efectores – alcanzar la “transparencia” del campo de batalla, que constituye una condición vital para la victoria en los conflictos actuales. En el campo de batalla ucraniano, la capacidad de combate de los contendientes depende de la acción combinada de su densa red de sensores, de su capacidad de transmitir información a sus servidores informáticos (donde es notable el papel decisivo de Star Link) y de la

capacidad de su IA de transformar los datos obtenidos en carpetas de objetivos y listas de “targeting”. Sin la IA, ningún equipo humano sería capaz de gestionar la enorme cantidad de información generada, lo que la haría inútil. Es decir, la disponibilidad de IA se convierte en una condición imprescindible para alcanzar la victoria, cuando no simplemente para tener posibilidades de supervivencia en el nuevo campo de batalla. De la misma forma, la operación en curso de norteamericanos e israelíes en Irán sería inviable sin el concurso de la IA.

Y esto, teniendo en cuenta que *todavía*, solo contamos con IA computacional y predictiva. Cuando se desarrolle una AGI, la influencia de la IA en la actividad militar será aún mayor y, consecuentemente, más decisiva.

Los debates éticos y morales que suscita el empleo de la IA con fines letales (que, al final, es lo que justifica la propia existencia de la “kill web” descrita) son cuestiones capitales que, a fecha de hoy, no están resueltos y que deberían suscitar un acuerdo transversal a los Estados que constituyen la sociedad internacional. El futuro de la Humanidad puede depender de que estos acuerdos se alcancen.

Bibliografía

- Gómez Pérez, Asunción (2024). “La Academia y la Inteligencia Artificial”. Madrid, Universidad Politécnica, 24 de septiembre.
- Martin Romero, Enrique y Gómez, Ángel (2026). *Inteligencia Artificial y Defensa*. Madrid, ed. Catarata.
- Rodríguez de Vallés, Eduardo (2026). “Empleo de la IA por las Fuerzas de Defensa de Israel en las acciones de fuego en la Guerra de Gaza (2023–2025).” Trabajo de Fin de Máster. Madrid, CESEDEN.
- U.S. Secretary of War (2026). *Artificial Intelligence Strategy for the Department of War*. Washington, 9 de enero.



CAPITULO SÉPTIMO

HONDURAS, COLEGIO DE DEFENSA NACIONAL

La influencia de las nuevas tecnologías en los escenarios futuros

Adán Antonio Ramírez Salinas
Nery Obdulio Mejía Espinoza
Rafael Antonio Maradiaga Molina

Acerca de los autores: Rector: El Coronel de Ingeniería Diplomado de Estado Mayor **Adán Antonio Ramírez Salinas** es licenciado en Ciencias Militares, entre su formación profesional destaca: Curso de Comando y Estado Mayor, Curso para Oficiales de Estado Mayor de las Naciones Unidas. Como militar se ha desempeñado como Comandante del primer Batallón de Ingenieros, Inspector General de la Policía Militar del Orden Público y Miembro de la Comisión Interventora del Instituto Nacional Penitenciario, actualmente es el Rector del Colegio de Defensa Nacional. Correo: lfpillajog@ejercito.mil.ec

Coordinador académico: El Coronel de Infantería D.E.M., Don **Nery Obdulio Mejía Espinoza** es licenciado en Ciencias Militares, entre su formación profesional destaca: el Curso Básico de Inteligencia, Curso de Seguridad Informática en el Centro de Adiestramiento del Buró de Seguridad Nacional de la República de China en Taiwán, Análisis de Inteligencia, curso de Altos Estudios Militares y especialidad en Altos Estudios Militares. Entre los cargos ocupados se encuentran: Director de la escuela de Inteligencia del Ejército, Director de la Escuela de Aplicación para Oficiales del Ejército, Director del Centro Penitenciario de Ilima Santa Bárbara, Jefe de División de Relaciones Interagenciales e Internacionales del Colegio de Defensa Nacional, actualmente es el Secretario General del Colegio de Defensa Nacional. Correo: nome1071@gmail.com

Rafael Antonio Maradiaga Molina: Doctor en ciencias de la Administración, Maestría en administración y finanzas, Ingeniero electricista Industrial, Ingeniero en telecomunicaciones, especialista en metodología de la investigación, estadística, tecnología de la información y comunicaciones; ciberdefensa y ciberseguridad. Actualmente docente del Colegio de Defensa Nacional de Honduras. Ingeniero electricista Industrial, docente en el Colegio de Defensa Nacional de Honduras. Correo: maradiagam@gmail.com

Introducción

Desde el principio de los tiempos el hombre ha evolucionado gracias a su ingenio y espíritu emprendedor, ha estudiado a través del tiempo el que, como, donde, porque de las cosas usando herramientas sofisticadas, de acuerdo a su época, que facilitan su vida, la forma de hacer negocios, la educación, la medicina, la astronomía, seguridad y defensa en fin una serie de disciplinas y especialidades en los campos de la ciencia a través de la aplicación de la tecnología.

Las redes de telecomunicaciones como plataformas de desarrollo de las tecnologías de información juegan un papel importante en las instituciones del Estado. Los sistemas de información son un componente clave, ya que este tipo de plataformas han evolucionado para favorecer y facilitar la toma de decisiones. El facilitar la comunicación, el procesamiento de datos y la manera de almacenar la información permiten establecer redes, y mediante los procedimientos adecuados. El simple hecho de escoger la tecnología adecuada a las condiciones y necesidades del entorno requiere un concienzudo análisis por los tomadores de decisiones. La tecnología, no es por sí misma la solución mágica a ninguna problemática. Se debe saber para qué queremos utilizarla y asegurarnos que cumplen expectativas de uso y calidad.

Las Tecnologías de la Información (TI) son una herramienta para facilitar la comunicación y la coordinación a distintos niveles a través de redes de telecomunicaciones. Los procesos de creación de conocimiento nunca deben iniciar ni terminar con la implementación de algún sistema de tecnologías de información y de ningún modo debe verse éste como el punto focal del proceso.

En este contexto, las Fuerzas Armadas de los países en desarrollo, enfrentan el reto de adaptarse a una nueva realidad operacional. Esta realidad exige ca-

pacidades tecnológicas robustas, interoperabilidad entre sistemas, vigilancia electrónica, ciber inteligencia y una arquitectura digital resiliente. La defensa nacional ya no depende únicamente del número de efectivos o de la capacidad bélica convencional, sino de la habilidad institucional para gestionar datos, proteger redes, interceptar amenazas digitales y garantizar la continuidad operativa mediante plataformas tecnológicas.

La incorporación de las TIC en los sistemas de defensa ha generado oportunidades significativas, tales como una mayor eficacia en la toma de decisiones, automatización de procesos, vigilancia satelital y análisis de inteligencia en tiempo real. No obstante, también ha expuesto a las instituciones de seguridad a nuevas formas de riesgo: ataques de ransomware, espionaje digital, sabotaje de infraestructuras¹ críticas, y desinformación masiva mediante plataformas digitales. Estos desafíos demandan una respuesta estratégica integral, basada en una inversión sostenida en tecnología, personal capacitado, y marcos legales adecuados. (Foro Económico Mundial, 2026)

Además de las guerras o conflictos armados a los que estamos acostumbrados, estaremos expuestos a influencias, riesgos y amenazas de todo tipo que se traducirán en un mayor número de disputas, mayor polarización social, menos consensos y más decisiones unilaterales de los que hemos presenciado en décadas anteriores. (Foro Económico Mundial, 2026)

Principales riesgos geopolíticos hasta 2026

La confrontación geoeconómica amenaza el multilateralismo: Ante la presión que sufre el consolidado sistema multilateral global, la confrontación geoeconómica se ha convertido en la principal preocupación de líderes y expertos en riesgos para 2026. Esto implica desafíos para el comercio, la inversión, las cadenas de suministro y el acceso a los recursos naturales. Además, ha relegado al segundo lugar el “conflicto armado entre estados”, que el año pasado ocupaba el primer puesto en la clasificación de riesgo.

¹ La infraestructura puede ser definida como las estructuras físicas y organizativas, redes o sistemas necesarios para el buen funcionamiento de una sociedad y su economía.

Si bien es posible que nos estemos acostumbrando a los aranceles, existe el riesgo de que la confrontación geoeconómica se convierta en una guerra económica a gran escala con bloqueos portuarios, restricciones a la exportación de productos clave, cancelación de contratos y controles de capital (Foro Económico Mundial, 2026)

Las condiciones meteorológicas extremas, la polarización social y la desinformación completan la lista de los cinco principales riesgos. La situación es similar en las perspectivas a dos años, que están encabezadas por la confrontación geoeconómica, la desinformación y la polarización social, mientras que el conflicto armado estatal ha descendido en la clasificación.

Sin embargo, desde una perspectiva de 10 años, la percepción del riesgo cambia sustancialmente. En este caso, las principales preocupaciones son los impactos del cambio climático, como los fenómenos meteorológicos extremos, la pérdida de biodiversidad y las alteraciones críticas en los sistemas terrestres. Entre las mayores preocupaciones para los próximos dos años, la desinformación y la información errónea también se perciben como un grave riesgo a largo plazo, ocupando el cuarto lugar, mientras que el temor a las consecuencias adversas de la IA completa los cinco primeros puestos. (Foro Económico Mundial, 2026)

Intensificación de los riesgos económicos: En comparación con el año pasado, los riesgos económicos muestran los mayores incrementos en la clasificación durante los próximos dos años. Junto con la confrontación geoeconómica, los riesgos de una recesión económica y la inflación experimentaron los mayores aumentos en gravedad y escalaron ocho posiciones. (Foro Económico Mundial, 2026)

Otro factor que experimentó un rápido ascenso fue el riesgo de que estallara la burbuja de activos, que subió siete puestos. Esto pone de manifiesto la volátil combinación que podría resultar de la interacción entre el aumento de la deuda, la recesión económica y la incertidumbre en la rentabilidad de las inversiones en tecnologías de vanguardia (IA, computación cuántica). Si a esto se le suma la confrontación geoeconómica, el impacto podría desestabilizar no solo a las empresas, sino a sociedades enteras, advierte el informe.

Riesgos tecnológicos sin control: La rápida evolución de tecnologías como la IA y la computación cuántica crea un terreno fértil para el crecimiento, pero también eleva los niveles de riesgo. Estos riesgos abarcan desde el impacto de la IA en el mercado laboral y la estabilidad social, a medida que los perfiles profesionales cambian radicalmente, hasta las dudas sobre la amenaza que la computación cuántica supone para la integridad de la información y los riesgos militares que plantean los sistemas de armas cada vez más automatizados. (Foro Económico Mundial, 2026).

La desinformación y la inseguridad cibernética ocupan el segundo y sexto lugar, respectivamente, en la proyección a dos años. Por su parte, los resultados adversos de la IA experimentan el mayor salto en la clasificación a lo largo del tiempo: del puesto 30 en el corto plazo al quinto en la proyección a diez años. Los resultados adversos de las tecnologías de vanguardia descienden del puesto 33 al 25 entre la proyección a dos y diez años. (Foro Económico Mundial, 2026).

La sensibilización, la educación, la reconversión profesional y las medidas de protección serán esenciales para las estrategias de mitigación.

La polarización social sigue siendo un factor de alto riesgo: Los riesgos de polarización social han sido un componente central y constante del panorama de riesgos globales durante las últimas cinco ediciones del Informe de Riesgos Globales.

Los riesgos sociales ocupan el tercer lugar en la proyección a dos años, descendiendo al noveno puesto cuando los encuestados analizan el panorama a diez años vista. Es el único riesgo que se ha mantenido entre los diez primeros en la lista de riesgos tanto a corto como a largo plazo durante los últimos cinco años. (Foro Económico Mundial, 2026).

La desigualdad, el deterioro de la salud y el bienestar, y la recesión económica están estrechamente interconectados con la polarización social. El Foro sugiere que, dado que aspectos como la desinformación y la confrontación geoeconómica también están interrelacionados, la polarización social y política podría profundizarse aún más en los próximos dos años.

Los riesgos ambientales disminuyen, pero siguen siendo elevados a largo plazo: Los riesgos ambientales han figurado entre los más prioritarios en los últi-

mos años. Sin embargo, este año se les está dando una nueva prioridad a corto plazo, en relación con amenazas no ambientales que se perciben como más urgentes. Si bien los fenómenos meteorológicos extremos y la contaminación aún se encuentran entre los diez primeros, con ligeros descensos en las previsiones para los próximos dos años, los cambios críticos en los sistemas terrestres y la pérdida de biodiversidad han experimentado un marcado descenso, situándose en la mitad inferior de la clasificación en comparación con el informe del año pasado. (Foro Económico Mundial, 2026)

El antiguo orden mundial se encuentra en un punto de inflexión: A medida que el proteccionismo y la política industrial estratégica van en aumento y los gobiernos asumen un control más activo de las cadenas de suministro críticas, el Informe de Riesgos Globales 2026 dibuja un panorama de un mundo “más competitivo”.

Se cree que, durante la próxima década, el entorno político mundial se volverá más fragmentado y multipolar. La posibilidad baja de espera para que se reactive el orden internacional de la posguerra y sus instituciones multilaterales, priorizando los intereses nacionales sobre la acción colectiva. (Foro Económico Mundial, 2026).

La infraestructura crítica está en riesgo crítico

En este panorama tan complejo, considero que los riesgos para las infraestructuras críticas —como la energía, el agua y los sistemas digitales— suelen subestimarse. La gente pasa por alto estos riesgos hasta que un incidente grave acapara los titulares.

El impacto de las condiciones climáticas extremas

El cambio climático ya está poniendo a prueba infraestructuras críticas de maneras que no se previeron cuando se diseñaron muchos sistemas. Las redes eléctricas se enfrentan a una creciente demanda de refrigeración al mismo tiempo que las olas de calor sobrecargan los equipos y reducen su eficiencia. La energía hidroeléctrica se enfrenta a riesgos de ambos extremos: las inundaciones pueden saturar y dañar las infraestructuras, mientras que las sequías

severas pueden detener la generación por completo. (Foro Económico Mundial, 2026).

La digitalización

La infraestructura sigue siendo un objetivo primordial en los conflictos, ocupando el quinto lugar en los próximos dos años. Los cables de comunicación submarinos pueden ser cortados; los satélites pueden ser interferidos; los drones pueden amenazar instalaciones críticas. El acceso a recursos esenciales —alimentos, agua, energía— puede ser utilizado como arma en disputas geopolíticas.

La digitalización está transformando esto en una amenaza híbrida, y la ciberseguridad figura entre los diez principales riesgos de la próxima década. Las infraestructuras conectadas, como las redes eléctricas, los puertos y los oleoductos, ofrecen una superficie de ataque más amplia tanto para grupos criminales como para actores vinculados a estados. Un ciberataque exitoso contra un sistema energético o una red de control de tráfico aéreo, por ejemplo, puede tener efectos en cascada mucho más allá del punto de fallo inicial, amplificando otras crisis físicas o geopolíticas.

La silenciosa crisis de infraestructuras

El Informe de Riesgos Globales también revela una brecha preocupante: todavía no prestamos suficiente atención a las amenazas sistémicas menos visibles que podrían resultar igualmente devastadoras, como, por ejemplo, el deterioro gradual de la infraestructura crítica, que requiere importantes reformas para seguir funcionando correctamente. Tomemos como ejemplo las redes eléctricas. En gran parte de la OCDE², estas son antiguas, carecen de recursos suficientes y son difíciles de modernizar o ampliar ante la creciente demanda. (Foro Económico Mundial, 2026).

² Organización para la Cooperación y el Desarrollo Económicos.

Parte del problema radica en otro riesgo subestimado: la insuficiencia de las finanzas públicas. Los riesgos económicos no figuran entre los 10 principales riesgos globales ni a dos ni a diez años vista, a pesar de que muchos gobiernos se enfrentan a una deuda creciente y de que los líderes empresariales encuestados en el Sondeo de Opinión Ejecutiva del Foro estaban preocupados por la amenaza de una recesión.

Cuando la economía flaquea, todos los demás riesgos se vuelven más difíciles de gestionar, incluidos los vinculados a la infraestructura crítica. La capacidad económica es más que un simple medio para financiar el mantenimiento y las mejoras esenciales; actúa como un amortiguador, ayudando a los países a reparar daños, invertir en prevención e impulsar las transiciones climática y digital. Del mismo modo, la infraestructura crítica está expuesta a una serie de riesgos, pero también sustenta nuestra capacidad para gestionar un espectro más amplio de amenazas.

La necesidad de una visión holística

Parte del problema radica en nuestra concepción del riesgo. Al centrarse en la crisis inmediata puede llevar a posponer medidas preventivas (como el mantenimiento) durante otro año. Con demasiada frecuencia, las perspectivas están fragmentadas. El clima y la sostenibilidad financiera, por ejemplo, a veces se tratan como cuestiones separadas y se abordan mediante estrategias distintas. Los riesgos que se perciben como más dramáticos —conflictos, pandemias, fenómenos meteorológicos extremos— suelen eclipsar amenazas menos evidentes, pero igualmente críticas.

Este enfoque fragmentado no tiene en cuenta una realidad fundamental: el espectro de riesgos globales está interrelacionado. El desafío que enfrenta la infraestructura crítica pone esto de manifiesto. Las tensiones geopolíticas, las disrupciones tecnológicas y la inestabilidad social convergen en los mismos sistemas subyacentes. Una red eléctrica sobrecargada por olas de calor también puede ser vulnerable a los ciberataques. Un puerto afectado por inundaciones puede amplificar las perturbaciones en la cadena de suministro y los disturbios sociales. La debilidad de las finanzas públicas limita la capacidad de mitigar o responder a cualquiera de estas amenazas.

En una era de competencia, nuestro instinto nos lleva a centrarnos exclusivamente en la crisis más reciente. Creo que el desafío —y la oportunidad— que deben afrontar los gobiernos y los responsables de la toma de decisiones reside precisamente en lo contrario: ampliar la perspectiva, observar cómo los riesgos se refuerzan mutuamente y diseñar soluciones de doble o múltiple uso que fortalezcan simultáneamente diversas dimensiones de la resiliencia.

Evolución de las TIC en los sistemas de defensa

Desde la Segunda Guerra Mundial hasta la actualidad, la tecnología ha sido un factor determinante en la superioridad militar de las naciones. La evolución de las tecnologías de la información y comunicaciones (TIC) ha marcado un antes y un después en la forma en que se conciben, planean y ejecutan las operaciones militares.

Estas se han estudiado en cuatro etapas, consideradas de la siguiente manera: (1) Las comunicaciones tradicionales (hasta finales del siglo XX), dependían de sistemas básicos, fundamentales en su época, eran limitados en cuanto a alcance y confiabilidad. En las décadas de 1950 y 1960, con el desarrollo de los sistemas de radar, la criptografía electrónica y los primeros ordenadores de propósito militar, se sentaron las bases de lo que hoy se considera la guerra digital. (2) La digitalización temprana (1980s-1990s), con la llegada de las primeras computadoras y sistemas de información, las fuerzas armadas comenzaron a digitalizar algunos de sus procesos. La digitalización de mapas, el uso de ordenadores en operaciones de comando y control, y la creación de bases de datos mejoraron significativamente, luego la comunicación por satélite, la integración de tecnologías capaces de crear información geográfica (GIS) y bases de datos de inteligencia.

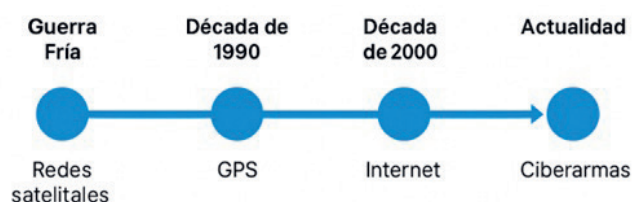


Figura 1. Línea de tiempo de la evolución de las TIC en el campo militar. Fuente: Propia del autor.

En las siguientes etapas: (3) Avances de redes y comunicaciones (2000s-2010s), la aparición de la internet y de redes globales mejoró la interoperabilidad de las fuerzas, los dispositivos móviles comenzaron a integrarse en el ámbito militar, permitiendo a las unidades en el terreno comunicarse y recibir órdenes con rapidez. Las aplicaciones de inteligencia militar y los drones empezaron a ser utilizados para recopilar datos y mejorar la vigilancia. Finalmente en la última etapa (4) La era de la inteligencia artificial y el ciberespacio (2020s-actualidad), la guerra cibernética y ciberdefensa se han convertido en un componente esencial de las operaciones militares, no solo para proteger las infraestructuras de información, sino también para realizar ataques, los sistemas autónomos, como los drones de combate, los robots militares y las armas autónomas, están cambiando la naturaleza del campo de batalla. (DOD, 2023)

Con la irrupción de la microelectrónica, los satélites de comunicación, y posteriormente el internet, las fuerzas armadas del mundo comenzaron a integrar capacidades tecnológicas más avanzadas, permitiendo la interconexión entre unidades dispersas geográficamente, el monitoreo en tiempo real de escenarios de combate y el acceso inmediato a inteligencia táctica y estratégica. A partir de los años 90, con la consolidación de la doctrina C4ISR³ las TIC dejaron de ser un mero soporte logístico para convertirse en un componente esencial de la defensa moderna. (Soriguera, 2023)

Hoy en día, la digitalización militar abarca desde simuladores de entrenamiento y drones no tripulados, hasta sistemas automatizados de defensa antimisiles y plataformas de guerra electrónica. (DOD, 2023)

La interoperabilidad entre ejércitos, alianzas estratégicas como la OTAN, y misiones de mantenimiento de paz han sido posibles gracias a protocolos de comunicación seguros, software militar especializado y redes protegidas por algoritmos criptográficos de última generación. Asimismo, los conflictos recientes han evidenciado que el dominio del ciberespacio es tan relevante como el dominio terrestre, aéreo o marítimo.

³ Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

No obstante, persisten retos estructurales como la dependencia de tecnología extranjera, el escaso presupuesto asignado a innovación militar, y la falta de una política nacional de defensa tecnológica que articule las prioridades de seguridad con una visión digital de largo plazo.

Esta evolución constante de las TIC en el ámbito de la defensa plantea una necesidad urgente de reformulación de estrategias, adopción de nuevas tecnologías emergentes como la inteligencia artificial y el big data, y la capacitación de personal militar especializado en operaciones cibernéticas. El rezago en esta materia no solo representa una vulnerabilidad operativa, sino también una amenaza directa a la soberanía e integridad del Estado.

Mando y control militar con apoyo de TIC

El concepto de mando y control (C2, por sus siglas en inglés) fundamental en las operaciones militares que se refiere al proceso de ejercer autoridad y dirección sobre las Fuerzas Armadas para alcanzar los objetivos establecidos en una misión o campaña; el mando es la autoridad conferida a un comandante para liderar y dirigir las fuerzas bajo su mando, y se basa en su capacidad para tomar decisiones que afecten a la operativa militar, implica la responsabilidad de la acción, la toma de decisiones estratégicas, tácticas y operacionales, y la capacidad de guiar y motivar a sus subordinados hacia el cumplimiento de los objetivos. El control también implica el monitoreo continuo del progreso de las operaciones, la evaluación de resultados y la adaptación a cambios inesperados o nuevas circunstancias.

Actualmente ha sido profundamente transformado por la incorporación de tecnologías de la información y las comunicaciones. Sin embargo, con la digitalización de los sistemas militares, este binomio ha evolucionado hacia estructuras más complejas y ágiles, agrupadas bajo el enfoque C4ISR, que integra elementos de inteligencia, vigilancia y reconocimiento, en conjunto con redes de comunicación y plataformas computacionales.

Actualmente está integrado por los siguientes componentes, los sistemas de mando y control militar operan en tiempo real, lo que permite una toma de decisiones más rápida y precisa, las TIC que han permitido el desarrollo de centros de comando conjuntos altamente digitalizados, en los cuales se inte-

gran datos provenientes de satélites, radares, sensores de campo, drones y sistemas de vigilancia marítima o aérea y ultimo elemento la cultura organizacional y liderazgo, esta capacidad de fusión de información posibilita la evaluación dinámica del campo de batalla, facilita la asignación eficiente de recursos y fortalece la coordinación entre unidades de tierra, mar y aire.

Entre los impactos claves de las TIC en este ámbito se encuentran: (1) La mejor comunicación y coordinación, brinda comunicación en tiempo real entre unidades geográficamente dispersas y con los distintos niveles de mando y ramas, empleando redes de comunicación modernas y seguras; (2) Inteligencia en tiempo real y análisis de datos, procesando información y preparando inteligencia del ambiente de operaciones con apoyo del IA, Big Data y análisis predictivo ayudando a tomar decisiones más informadas, predecir movimientos enemigos y optimizar las tácticas.

Otros impactos a considerar son:(3) Descentralización del mando y Control, dando cabida a su iniciativa de combate con elecciones más rápidas y autónomas, dando sistemas de C2 integrados con autonomía y flexibilidad, generando situaciones más dinámicas aumentando las posibilidades de éxito en la ejecución de las misiones.



Figura 2. Estructura de sistema C-2 militar asistido por TIC. Fuente: Propia del autor.

También se contemplan como parte del impacto a: (4) Ciberseguridad y Defensa Cibernética, generando una nueva dimensión en el conflicto, teniendo que realizar protección de infraestructuras críticas como lo son ahora los Centros de Datos, donde se encuentran los servidores, sistemas de control y los equipos tecnológicos que protegen de los ataques cibernéticos, el desarrollo de herramientas de guerra cibernética, como el hacking de sistemas enemigos y el uso de software malicioso, se ha integrado a las estrategias militares para desestabilizar las comunicaciones y los sistemas de mando del adversario.

Se debe considerar como segmento del impacto a: (5) Simulaciones y Capacitación Avanzada, permitiendo entrenar a las tropas en situaciones complejas y realistas sin necesidad de estar físicamente en el campo de batalla.; (6) Integración de Fuerzas Multidominio y Multinacionales, donde las fuerzas aéreas, navales, terrestres y cibernéticas trabajan en conjunto permitiendo la interoperabilidad entre los ejércitos de diferentes países, donde las TIC permiten coordinar todas las áreas operacionales (tierra, aire, mar, ciberespacio y dominio espacial) para que trabajen en conjunto hacia un objetivo común. (Pérez & Rodríguez, 2022)

El software especializado en planificación táctica, los sistemas de gestión de operaciones (Battle Management Systems) y los simuladores de escenarios de conflicto han redefinido los procesos de comando. Las TIC permiten hoy el modelado predictivo, la evaluación de múltiples cursos de acción, y la retroalimentación inmediata basada en indicadores de desempeño operacional. Esto ha reducido la dependencia de las jerarquías rígidas y ha promovido esquemas de mando más descentralizados, flexibles y adaptativos.

La creciente dependencia de los sistemas de información y la digitalización de las operaciones militares está transformando profundamente las estructuras de defensa y seguridad nacional. Esta tendencia ha impactado tanto la manera en que las Fuerzas Armadas planifican, ejecutan y coordinan operaciones, como la manera en que se protegen y gestionan los recursos estratégicos del país.

Entre las implicaciones más importantes de esta dependencia se encuentran: (1) La transformación de las capacidades y de la toma de decisiones, permitiendo una mejor gestión de los recursos, la optimización de las operaciones y la toma de decisiones más rápidas e informadas.; (2) Incremento de la vulne-

rabilidad a ciberamenazas, desarrollando guerra cibernética para deshabilitar las infraestructuras críticas de mando y control, alterar comunicaciones, manipular datos de inteligencia o incluso comprometer armas y equipos militares, así como ataques a infraestructuras críticas.

De igual manera se encuentran estas implicaciones: (3) Interoperatividad y Cooperación Internacional, manteniendo plataformas de comunicación compartidas, coordinando operaciones conjuntas con estándares comunes entre todos los participantes.; (4) Dependencia de la infraestructura digital y riesgos en el medio de conflictos, Si los sistemas de comunicación y control se ven comprometidos, la resiliencia de las operaciones puede verse afectada. A medida que la información se digitaliza y circula más rápido, los actores hostiles pueden intentar inundar las redes con desinformación o noticias falsas para desestabilizar la percepción pública y política, lo cual afecta la toma de decisiones y el apoyo social a las políticas de seguridad.

Así mismo acompañan a estas implicaciones, (5) Optimización de la logística y el suministro, permiten gestionar y optimizar la distribución de suministros, el mantenimiento de equipos y la gestión de inventarios en tiempo real, así como el rastreo de los recursos críticos, asegurando que las unidades tengan todo lo que necesitan sin interrupciones.

Ciberseguridad y defensa cibernética

La ciberseguridad y la defensa cibernética constituyen hoy en día uno de los pilares estratégicos más importantes en el ámbito de la seguridad y defensa nacional, (World Economic Forum, 2023).

A medida que las Fuerzas Armadas, los organismos gubernamentales y las infraestructuras críticas dependen crecientemente de sistemas informáticos interconectados, también aumentan exponencialmente los riesgos asociados a ciberataques, espionaje digital, sabotajes electrónicos y operaciones de desinformación.

En el plano nacional, proteger los activos digitales esenciales —como sistemas de mando y control, bases de datos militares, redes de telecomunicaciones, satélites, y sistemas de logística y abastecimiento— es fundamental para ga-

garantizar la soberanía y la estabilidad. Los ataques de denegación de servicio (DDoS), el secuestro de datos mediante ransomware, la intrusión en redes mediante malware avanzado o el acceso no autorizado a información clasificada representan amenazas reales que ya han afectado a múltiples Estados en el mundo, (WOLA, 2020).

La defensa cibernética, como componente integral de la seguridad nacional, va más allá de las soluciones técnicas y exige una arquitectura institucional sólida. Esto implica la existencia de organismos especializados como centros de operaciones de ciberseguridad (SOC), equipos de respuesta ante incidentes cibernéticos (CSIRT), cibercomandos militares, legislación específica y políticas públicas orientadas a la protección del ciberespacio soberano.

En países como Estados Unidos, Israel y Estonia, las capacidades de defensa cibernética se consideran parte del aparato militar, equiparándose a las fuerzas terrestres, navales y aéreas, (UNODA, 2022).

Uno de los principales desafíos es la formación y retención de talento humano, la escasez de profesionales en ciberseguridad, la fuga de cerebros al sector privado y la limitada capacidad de los institutos militares y civiles para formar expertos altamente cualificados, reducen la capacidad operativa del país. Además, la debilidad en políticas de ciberhigiene institucional, la baja inversión en infraestructura de monitoreo y la falta de planes de continuidad del negocio ante ataques cibernéticos comprometen la resiliencia del Estado.

La ciberseguridad no puede concebirse como una responsabilidad exclusiva del sector militar o gubernamental, sino como un esfuerzo articulado entre todos los actores que operan en el entorno digital nacional.

Las TIC han abierto un nuevo campo de operaciones en el ciberespacio, el cual requiere un enfoque integral, interdisciplinario y actualizado para proteger la seguridad nacional. La defensa del ciberespacio es hoy una extensión del territorio soberano y, como tal, debe ser vigilado, protegido y defendido con la misma prioridad que las fronteras físicas del país, (CEPAL, 2021).

Interoperabilidad, integración y transformación digital

La transformación digital en el ámbito de la defensa y la seguridad nacional representa un cambio estructural que redefine cómo operan, comunican y toman decisiones las instituciones encargadas de proteger la soberanía. En este proceso, la interoperabilidad emerge como un factor esencial para lograr una coordinación efectiva entre los diferentes componentes de las Fuerzas Armadas, organismos civiles, agencias de inteligencia y aliados internacionales.

La interoperabilidad no se limita a la compatibilidad técnica de sistemas; implica la capacidad de compartir información de manera segura, oportuna y estandarizada, integrando plataformas heterogéneas en un entorno común de operaciones. En escenarios de defensa moderna, como desastres naturales, amenazas híbridas o conflictos asimétricos, la sincronización de recursos y datos en tiempo real es determinante para la eficacia de la respuesta, (Sandoval, 2021).

La transformación digital, sin embargo, va más allá de integrar sistemas. Implica repensar procesos internos, modernizar infraestructuras, adoptar tecnologías emergentes (como inteligencia artificial, big data, computación en la nube y sensores IoT), capacitar al personal y fomentar una cultura de innovación. Esta transición, si es bien ejecutada, permite mejorar la eficiencia, transparencia y capacidad de adaptación de las instituciones de seguridad, (IDB, 2020).

Un aspecto clave en esta transformación es el desarrollo de centros de mando y control digitalizados, capaces de recopilar datos desde múltiples fuentes (inteligencia, vigilancia, sensores de campo, comunicaciones civiles), analizarlos en tiempo real y apoyar la toma de decisiones estratégicas con dashboards integrados. Asimismo, el uso de sistemas de gestión del conocimiento permitiría retener experiencias operacionales, lecciones aprendidas y planes de contingencia frente a amenazas futuras.

Impulsar la interoperabilidad e integración tecnológica requiere una política de Estado que establezca lineamientos técnicos, jurídicos y presupuestarios. Es necesario crear un marco regulatorio de interoperabilidad nacional, fortalecer las capacidades del Instituto Nacional de Estadística y de las instituciones TIC del gobierno, e integrar gradualmente a las Fuerzas Armadas a una red nacio-

nal segura basada en protocolos cifrados y tecnologías modernas. La inversión en plataformas abiertas, escalables y sostenibles a largo plazo es vital para no depender de soluciones propietarias o vulnerables a obsolescencia rápida.

Infraestructura crítica

Los sectores que componen la clasificación de infraestructura crítica⁴ de cada sector son muy similares y se repiten en varias clasificaciones a nivel internacional, mientras se adopta una política específica para infraestructuras críticas, la infraestructura de la información de los siguientes sectores será considerada como crítica:

- Sector administración pública,
- Sector energético,
- Sector telecomunicaciones,
- Sector agua,
- Sector salud,
- Sector servicios financieros,
- Sector protección civil y defensa,
- Sector seguridad pública,
- Sector transporte,
- entre otras.

La política de infraestructuras críticas contendrá un esquema acabado de áreas, funciones y entidades estatales responsables que servirán para identificar y delimitar el nivel crítico de cada sector.

Los órganos técnicos encargados de ejecutar medidas que se deriven de la presente política, deberán considerar estándares especiales de ciberseguridad, atendido sus particulares niveles de madurez, para las infraestructuras críticas, especialmente respecto a sus procesos esenciales.

⁴ La infraestructura crítica se refiere a los sistemas y activos físicos o virtuales esenciales para el funcionamiento de la sociedad y la economía.

En el mediano plazo se avanzará en desarrollo de medidas que garanticen la continuidad de servicio mediante redundancia de instalaciones físicas de algunas infraestructuras críticas, especialmente en los sectores de energía, telecomunicaciones, administración pública, protección civil y defensa.

Ataques contra la infraestructura crítica

Las infraestructuras críticas esenciales para el buen funcionamiento de la sociedad (energía, agua, transportes, logística alimentaria, telecomunicaciones, bancos y servicios financieros, servicios médicos, funciones gubernamentales, etc.), resultan más vulnerables por su creciente utilización de las tecnologías de internet que permiten el acceso a las mismas desde la red de redes.

Además, es necesario subrayar la importancia particular de la vulnerabilidad de los sistemas de producción y distribución de electricidad. Éstos constituyen una infraestructura vital, y por lo tanto, crítica, en la medida en que condiciona el funcionamiento de la mayor parte de las demás infraestructuras. La complejidad y el carácter distribuido de las relaciones entre las distintas infraestructuras críticas es a la vez causa de fuerza y de vulnerabilidad.

Es fundamental asegurar las pasarelas hacia internet de las redes de gestión de estas infraestructuras y crear, ya sea a nivel regional o nacional, organismos encargados de la protección de las infraestructuras críticas, cuya misión principal sea la de coordinar la concepción y actualización de los planes de protección de cada una de estas infraestructuras.

Efectivamente, la coherencia y compatibilidad de estos planes y soluciones de seguridad son de carácter primordial en caso de crisis que afecte simultáneamente a varias de ellas.

Organización para la infraestructura crítica

Los activos nacionales críticos son definidos como sistemas y bases de datos que son esenciales para la misión operacional y procesos de la organización, la lista de activos críticos a nivel nacional, es el resultado de mapear y analizar los servicios nacionales, junto con la experiencia acumulada de definiciones similares a nivel mundial:

Infraestructura crítica	· Sistema de gestión de la red eléctrica. · Sistema de gestión de la red de agua. · Cadena de suministro del sistema de gas y petróleo. · Sistema de salud.
Seguridad nacional	· Sistemas operacionales en uso por agencias de Defensa y Orden Público. · Sistema de Inteligencia nacional.
Gobierno y gobernanza	· Sistema de identificación nacional. · Sistema de control de fronteras. · Sistema de registro de propiedades. · Sistema de información del Congreso. · Sistema de recuperación de desastres naturales. · Bases de datos nacionales. · Sistema de información nacional que soporta eventos especiales y mega eventos (elecciones, deportes, visitas).
Financiero	· Sistema central bancario y sistema del sector financiero. · Sistema unificado de procesamiento de impuestos.
Telecomunicaciones	· Infraestructura de telecomunicaciones. · Puntos de intercambio de Internet (IXP). · Sistema de nombre de dominio nacional.
Transporte	· Sistema de torres de control aéreo. · Sistema de control de radares de tráfico aéreo nacional. · Sistema de control marítimo. · Sistemas meteorológicos.

Protección de la infraestructura crítica

La responsabilidad principal y última de proteger las Infraestructuras Críticas corresponde al Estado y las instituciones que la componen, así como a los propietarios u operadores de tales infraestructuras que aportan al desarrollo económico y social.

Dado que aquellos sectores que cuentan con una especial experiencia, desarrollo y pericia, y tienen también necesidades particulares en materia de protección de infraestructuras críticas, deben desarrollar y aplicar un planteamiento local en pro del beneficio comunitario de protección de infraestructuras críticas teniendo en cuenta las características específicas de los diferentes sectores y las medidas sectoriales existentes, como las ya vigentes en cada uno de las localidades a la cual pertenecen a escala comunitaria, nacional o regional. (Consejo de la Unión Europea, 2008).

Habida cuenta de la significativa experiencia del sector privado en el control y gestión de riesgos, en la planificación de la continuidad de las actividades y en

la recuperación después de una catástrofe, el planteamiento comunitario debe fomentar la plena participación de dicho sector.

Sin duda, uno de los mayores problemas asociados a la protección de las infraestructuras críticas es la complejidad de lo que se viene a llamar el ecosistema; existen muchos agentes involucrados en dicha protección, y por tanto la coordinación y la comunicación entre ellos debe ser ágil y segura para garantizar la seguridad de estas infraestructuras.

La seguridad de las infraestructuras críticas debe garantizarse desde cualquier punto de vista; la seguridad es un concepto global, y el medio natural, un atacante —cuyo objetivo, no lo olvidemos, es dañar a sus víctimas—o un accidente simplemente elegirá el camino más fácil para materializarse.

La probabilidad de un ciberataque contra infraestructuras críticas es más que significativa, por lo que hay que tomar medidas para reducir el riesgo asociado a estas amenazas.

Planificación sectorial de la infraestructura crítica

En todas las Infraestructuras Críticas designadas deben existir planes de seguridad del operador o medidas equivalentes que incluyan la identificación de los elementos importantes, una evaluación de riesgos y la identificación, selección y orden de preferencia de las contramedidas y procedimientos. (Consejo de la Unión Europea,, 2008)

A fin de evitar trabajos inútiles y duplicidad de esfuerzo, cada sector involucrado debe evaluar en primer lugar si los actores del sector privado y público de las Infraestructuras Críticas designadas tienen planes de seguridad.

Debe considerarse que las medidas, principios y directrices —incluidas las medidas comunitarias— así como los planes de cooperación bilaterales o multilaterales que prevean planes similares o equivalentes al plan de seguridad del operador o responsables de enlace para la seguridad o equivalentes, cumplen los requisitos que impone la planificación establecida por el Estado en relación respectivamente con el plan de seguridad del operador o el responsable de enlace para la seguridad.

Se ha de nombrar responsables de enlace para la seguridad para todas las Infraestructuras Críticas con el fin de facilitar la cooperación y la comunicación con las autoridades nacionales responsables de la protección de infraestructuras críticas, (Consejo de la Unión Europea, 2008).

Confidencialidad de la información de la infraestructura crítica

El intercambio de información sobre las Infraestructuras Críticas debe producirse en un entorno de confianza y seguridad.

Este intercambio requiere una relación de confianza en la que empresas y organizaciones sepan que sus datos sensibles y confidenciales estarán suficientemente protegidos, (Consejo de la Unión Europea, 2008).

Actores según sector

El elevado número de actores involucrados en la seguridad de las infraestructuras críticas no debe ser un obstáculo para protegerlas; así, es necesario potenciar la colaboración y el intercambio de información entre los actores participantes en la PIC nacional a diferentes niveles, desde el estratégico al operativo, y también con diferentes ámbitos de colaboración:

Actores del ámbito público: El intercambio de información entre entidades del ámbito público debe ser garantizado al más alto nivel; la implicación de múltiples actores debe ser liderada en la práctica de forma única y coordinada, evitando que los ámbitos de competencia de cada uno de ellos se conviertan en un obstáculo para la capacidad de respuesta nacional.

Actores del ámbito privado: Dado el considerado porcentaje de infraestructuras críticas operadas por el sector privado, la participación de este en cualquier iniciativa de seguridad es clave para garantizar el éxito de la misma y si a este hecho añadimos la interdependencia entre infraestructuras, la relevancia del sector privado es aún mayor. En este caso los obstáculos a superar vienen marcados por el recelo a la colaboración que en ocasiones puede producirse entre organizaciones que en casos son incluso competencia, y en este sentido las empresas deben abandonar la idea de seguridad como diferencia o negocio y adoptar la estrategia de "*responsibility to provide*".

Colaboración público-privada: La coordinación entre el ámbito público y privado para la protección de infraestructuras críticas debe ser también exhaustiva, constituyendo lo que se viene a denominar PPP (*Public-Private Partnerships*) y garantizando que los esfuerzos son comunes y van siempre en la misma dirección.

El marco de esta colaboración debe extenderse a todos los ámbitos de la seguridad de una infraestructura crítica; en el marco de la seguridad privada la colaboración y el intercambio de información con la seguridad pública es algo habitual, e incluso lo es —cada vez más— entre empresas o Departamentos de Seguridad que en muchos casos son competencia directa. Cuando hablamos de protección lógica el panorama es completamente diferente: si bien la colaboración público privada es común, no lo es tanto la colaboración entre empresas o actores exclusivamente del sector privado, y esto claramente perjudica al global de la seguridad nacional.

Un enfoque piramidal, en el que desde la cima —la estrategia— hasta la base —la operativa— se definan y articulen los mecanismos de protección al nivel correspondiente. Cualquier iniciativa que no venga liderada y apoyada desde el propio Estado y con el más alto nivel estará condenada al fracaso.

Como también lo estará cualquier iniciativa que, como antes hemos dicho, focalice su atención en unas amenazas concretas y descuide otras en función de en qué ámbito se puede materializar cada una de ellas.

Desde el punto de vista técnico es necesario reforzar la seguridad en entornos de control industrial asociados a las infraestructuras críticas, sistemas que o bien se diseñaron para trabajar en entornos aislados, sin considerar amenazas provenientes de la otra punta del mundo, o bien están a cargo de equipos que no tienen la idea de la interconexión de sistemas en la cabeza.

En la protección de infraestructuras críticas actual desde el punto de vista lógico debemos aplicar, a muy corto plazo, medidas drásticas que incrementen la seguridad tecnológica de las infraestructuras, en especial la de los sistemas de control industrial, en dos grandes líneas: control de acceso y robustez de aplicaciones; algo similar a las medidas que en su momento se tomaron para proteger los sistemas generalistas, expuestos a internet por completo.

Infraestructura crítica, brecha digital y capacidades del Estado

La defensa y seguridad nacional no pueden analizarse de forma aislada de la infraestructura crítica que sostiene el funcionamiento del país. La infraestructura crítica comprende los sistemas, activos y servicios esenciales cuya interrupción afectaría significativamente la seguridad, la economía, la salud pública o el bienestar social. Esta categoría incluye las telecomunicaciones, la energía eléctrica, el suministro de agua, las redes de transporte, las instituciones financieras, los servicios de emergencia, y cada vez más, los sistemas informáticos y plataformas digitales del gobierno, (Consejo de la Unión Europea, 2008).

La protección de estas infraestructuras representa un desafío central en la estrategia de seguridad nacional, especialmente en una era donde las amenazas físicas y cibernéticas se entrelazan. Ciberataques a centrales eléctricas, sabotajes digitales a sistemas de comunicación militar o vulneraciones a bases de datos gubernamentales pueden tener efectos tan devastadores como un ataque convencional. Por ello, la resiliencia de la infraestructura crítica debe ser entendida como un componente de la capacidad defensiva del Estado.

Sin embargo, uno de los mayores obstáculos para fortalecer esta resiliencia es la brecha digital, tanto geográfica como institucional. Mientras que algunas áreas urbanas cuentan con acceso a tecnologías modernas, conectividad estable y plataformas gubernamentales parcialmente automatizadas, extensas regiones rurales permanecen desconectadas, lo que limita la cobertura y eficacia de cualquier estrategia de defensa territorial integral. Asimismo, muchas instituciones públicas carecen de equipos adecuados, personal capacitado en ciberseguridad y protocolos básicos de respaldo o continuidad operativa.

En esta realidad no es difícil admitir que en esta era del conocimiento, las diferencias no se establecerán entre ricos y pobres, sino entre alfabetos -los conectados a la red- y los que no lo están, las analfabetas. No hay competitividad sin conectividad, que por sí sola no es suficiente.

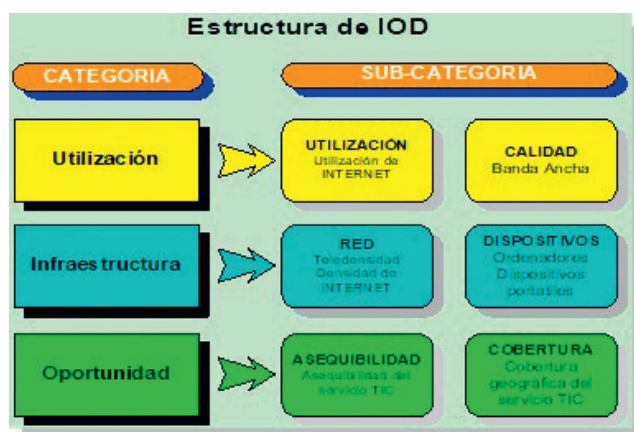


Figura 3. Estructura de IOD. Fuente: Adaptado de C.M. Cho, Actualidades UIT (2025).

La expansión rápida de la sociedad de la información puede también tener efectos negativos. Puede agravar las disparidades económicas existentes a nivel internacional, regional y local. El acceso a las TIC y su disponibilidad, así como la capacidad de utilizarlas pueden ser consideradas como una amenaza por aquellos que no las poseen. El principio de acceso sin discriminación a los servicios modernos de telecomunicación es importante para colmar la brecha.

Se propone la diversidad digital, establecida por el "índice de oportunidad digital" (IOD), creado por la UIT que contiene indicadores aprobados a escala internacional y sirve para evaluar la situación de las TIC en cada país, evalúa éxito o fracaso de sus iniciativas tecnológica con respecto a otros países. y, por consiguiente, mide el acceso a la sociedad de la información.

La brecha digital institucional se evidencia en la fragmentación de bases de datos, la falta de interoperabilidad entre plataformas del gobierno, el uso de software obsoleto o pirata, y la ausencia de políticas claras de ciberdefensa. Esto no solo vulnera la privacidad de la información estatal, sino que dificulta la acción coordinada ante crisis de origen natural o intencional. (Unión Internacional de Telecomunicaciones, 2002).

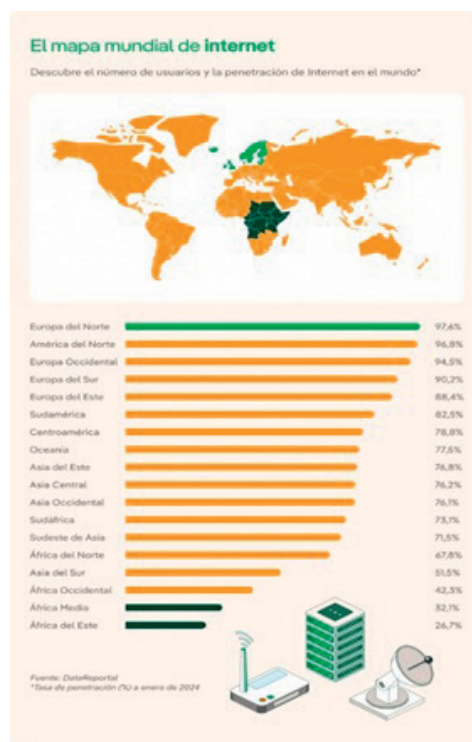


Figura 4. Desigualdad del acceso al internet en el mundo. Fuente: IBERDROLA / 2024.

Desde una perspectiva estratégica, el fortalecimiento de la infraestructura crítica y la reducción de la brecha digital deben ser entendidas como pilares complementarios. Para ello, el Estado necesita incrementar su capacidad operativa y técnica, mediante: (1) Inversiones sostenidas en tecnología de comunicaciones seguras (como redes LTE tácticas, enlaces satelitales redundantes y nodos de datos blindados).; (2) La creación de un Centro Nacional de Ciberseguridad e Infraestructura Crítica, con participación civil-militar, que vigile, coordine y mitigue riesgos asociados a ataques físicos y digitales.

De igual manera, (3) El impulso a programas de conectividad universal, que integren a las regiones más aisladas a la red nacional de vigilancia y comunicaciones. (4) La capacitación continua de funcionarios públicos, militares y cuerpos de seguridad en gestión de tecnologías críticas y respuesta a incidentes.



Figura 5. Creación del conocimiento. Fuente: Propia del autor.

A pesar de que la introducción de nuevas tecnologías de información, beneficia a países de más bajo perfil tecnológico e infraestructura en las redes de telecomunicaciones en comparación con a países con la globalización de la información, los perjuicios que conllevan son mucho mayores. Dicho fenómeno es particularmente notable en el ámbito informativo y económico con la introducción de Internet de los países industrializados hacia los que están en vías de industrialización, ya que estos se han convertido en consumidores de discursos creados por primermundistas, y han tenido que adaptarse a las transacciones de comercio electrónico diseñadas y operadas por los países con la infraestructura para manejar la economía mundial.

Además, el desarrollo de planes nacionales de continuidad operativa, que incluyan simulacros, auditorías y análisis de riesgo integral, es vital para garantizar que las operaciones del Estado no se interrumpan ante escenarios adversos. Estos planes deben contemplar tanto la redundancia técnica como la distribución geográfica de los centros de datos y capacidades logísticas.

La inclusión digital, sostiene este sector de la sociedad civil, hay que pensarla como un asunto colectivo, no individual, donde los beneficios sociales hay que verlos en relación a los que se generan para las comunidades, organizaciones, familias y grupos que sacan provecho de las tecnologías, aunque no tengan acceso a éstas

La creación del conocimiento es un arduo proceso que implica un compromiso a todos los niveles, así como una participación y responsable de los diversos

actores de la sociedad, las tecnologías de información son uno de los componentes claves para alcanzar cada una de las etapas involucradas en la creación del conocimiento.

Las TIC por sí mismas sólo se consideran como una herramienta para facilitar la comunicación y la coordinación; los procesos de creación de conocimiento nunca deben iniciar ni terminar con la implementación de algún sistema de TIC y de ningún modo debe verse éste como el punto focal del proceso, (Nonaka, 1995).

Ética, legislación y soberanía digital en el uso de TIC para la seguridad nacional

El uso de tecnologías de información y comunicación (TIC) en la defensa y seguridad nacional plantea dilemas complejos que van más allá de la eficacia técnica. La ética, el marco legal y el respeto a la soberanía digital son elementos indispensables para asegurar que las herramientas digitales no se conviertan en instrumentos de abuso, vigilancia arbitraria o pérdida del control nacional sobre los sistemas críticos.

Ética y derechos fundamentales

En una democracia, las TIC deben emplearse bajo principios éticos que resguarden los derechos humanos, la privacidad y las libertades individuales. La instalación de cámaras de vigilancia, el monitoreo de redes sociales, la interceptación de comunicaciones o el uso de inteligencia artificial para identificar amenazas deben estar sujetos a límites proporcionales, supervisión independiente y mecanismos de rendición de cuentas. El riesgo de que estos sistemas se utilicen para controlar políticamente a la población o perseguir a opositores es real, como ha ocurrido en regímenes autoritarios que han adoptado tecnologías de vigilancia masiva sin controles.

Conclusiones

La transformación digital de los sistemas de defensa nacional no es una opción, sino una necesidad impostergable. Las Tecnologías de la Información y las Comunicaciones (TIC) han redefinido la forma en que se conciben y ejecutan las operaciones militares, la inteligencia estratégica, la seguridad interna y la protección de infraestructuras críticas. Del análisis realizado se concluye que:

1. Las TIC han transformado las estructuras tradicionales de mando y control en las Fuerzas Armadas, permitiendo una gestión más eficiente de las operaciones militares, un mejor acceso a la información, mayor autonomía para los mandos de campo, y una respuesta más rápida ante situaciones cambiantes.
2. Las TIC son un componente transversal y estratégico para la defensa nacional, ya que habilitan sistemas de mando y control efectivos, permiten la interoperabilidad de fuerzas y optimizan la toma de decisiones en tiempo real.
3. A medida que las tecnologías continúan evolucionando, el impacto de las TIC sigue ampliándose, promoviendo operaciones militares más dinámicas, interoperables y adaptables.
4. La ciberseguridad se posiciona como uno de los principales frentes de defensa del siglo XXI. Las Fuerzas Armadas requieren estructuras formales de defensa cibernética, tanto para protegerse de ataques como para disuadir a actores hostiles, estatales o no estatales.
5. Los ciberataques, la interferencia en las comunicaciones, la desinformación, la falta de redundancia y las amenazas a las tecnologías autónomas son algunos de los mayores desafíos que enfrentan las Fuerzas Armadas y las instituciones de seguridad nacional en este contexto.
6. La ciberseguridad, la resiliencia en la infraestructura digital y la formación continua son cruciales para mitigar los riesgos y proteger la integridad de las operaciones militares en un entorno cada vez más digitalizado.
7. Existe una deuda estructural en inversión, normativa y talento humano, que limita el desarrollo tecnológico militar y reduce la soberanía digital del país. El retraso en infraestructura, capacitación y doctrina digital constituye una vulnerabilidad estratégica.

8. El futuro de las TIC en el mando y control de la defensa y seguridad nacional estará marcado por la automatización, la inteligencia artificial, la ciberseguridad avanzada y la interoperabilidad global.
9. La cooperación regional y el fortalecimiento institucional interno son factores claves para una defensa moderna. Solo mediante alianzas tecnológicas, normativas claras y una visión de Estado será posible integrar un ecosistema de seguridad global robusto y confiable.
10. Esta transformación requiere que las Fuerzas Armadas no solo inviertan en tecnologías avanzadas, sino también en la protección de sus infraestructuras digitales y en la capacitación de su personal para adaptarse a este nuevo entorno digital.
11. El aprovechamiento de las TIC en la defensa nacional hondureña debe partir de una visión integral, donde la tecnología no se conciba como un simple recurso operativo, sino como un eje de transformación institucional, doctrinal y estratégica.
12. La interoperabilidad y la transformación digital son condiciones indispensables para una defensa nacional moderna, eficiente y resiliente. Su implementación permitirá mejorar la coordinación interinstitucional, responder con agilidad a amenazas emergentes y participar de manera más efectiva en misiones multilaterales y alianzas internacionales.

Bibliografía

- CEPAL. (2021). *Comisión Económica para América Latina y el Caribe. La ciberseguridad como un desafío para América Latina y el Caribe*. CEPAL.
- CNDS. (2018). *Política Nacional de Defensa y Seguridad. Gobierno de Honduras. Política Nacional de Defensa y Seguridad. Funciones y atribuciones*. Tegucigalpa, Francisco Morazán, Honduras: La Gaceta.
- Consejo de la Unión Europea,. (2008). *sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la*. DIRECTIVA 2008/114/CE DEL CONSEJO.
- DOD. (2023). *Cyberspace Strategy Report*. DOD.

- Foro Económico Mundial. (2026). *Informe sobre riesgos globales 2026*. Coligny/ Geneva: WEF. Obtenido de <https://www.weforum.org/publications/global-risks-report-2026/>
- IDB. (2020). *Cybersecurity risks, progress, and the way forward in Latin America and the Caribbean*. IDB.
- Navas, A. Á. (1 de Septiembre de 2022). La nueva Ley de Seguridad y Defensa Nacional: equilibrios de poder y fortalecimiento del estado de derecho en Honduras. *La nueva Ley de Seguridad y Defensa Nacional: equilibrios de poder y fortalecimiento del estado de derecho en Honduras*. doi:Criterio.hn.
- Nonaka, I. T. (1995). *The Knowledge-Creating Company*. USA: Oxford University Press.
- OEA. (2021). *Estado de la ciberseguridad en América Latina*. . OEA.
- Pérez, J. A., & Rodríguez, M. (2022). Infraestructura crítica y ciberseguridad en el contexto de la seguridad nacional. *Revista de Estudios en Seguridad y Defensa*, 10(2), pp. 45-67.
- Sandoval, C. (2021). Mando y control militar en la era digital: una perspectiva latinoamericana. *Revista Seguridad & Defensa*, 8(1), 31-48.
- Soriguera, M. S. (2023). Nuevas tecnologías en el contexto global de seguridad: la oportunidad frente al desafío. *Instituto Español de Estudios Estratégicos (IEEE)*. , 75/2023.
- Unión Internacional de Telecomunicaciones. (2002). *Conferencia Mundial de desarrollo de las Telecomunicaciones*. Final, UIT, CMDT-02, Estambul, Turquía.
- UNODA. (2022). (2022). *Developments in the field of information and telecommunications in the context of international security*. . ONU.
- WOLA. (2020). *El papel de las Fuerzas Armadas en la seguridad pública en Honduras. Evaluando la limitación de las Fuerzas Armadas en funciones policiales*. UNAH.
- World Economic Forum. (2023). *Global Cybersecurity Outlook*. Obtenido de Global Cybersecurity Outlook: <https://www.weforum.org/reports/global-cybersecurity-outlook-2023>



CAPÍTULO OCTAVO

MÉXICO, CENTRO DE ESTUDIOS SUPERIORES NAVALES (CESNAV)

Tecnologías disruptivas y su impacto en la seguridad global de los Estados: un nuevo paradigma

David Sánchez Hernández (Ph.)
Francisco Chávez Gutiérrez (Ph.)

Resumen: El siglo XXI ha traído consigo una revolución tecnológica que está redefiniendo los cimientos mismos de lo que entendemos por seguridad nacional. Este trabajo examina cómo diez tecnologías clave, desde la inteligencia artificial hasta los avances en biotecnología y el espacio, están alterando los escenarios operativos futuros, las dinámicas de poder internacional y la capacidad de los Estados para proteger su soberanía. A través de un análisis que cruza dimensiones políticas, económicas, sociales, militares, tecnológicas, diplomáticas y ambientales, el estudio argumenta que la autonomía tecnológica se ha convertido en un pilar fundamental de la seguridad nacional moderna. Se identifican riesgos estratégicos emergentes, así como oportunidades para fortalecer las instituciones estatales, y se plantean tres posibles escenarios de evolución hacia 2035. Las conclusiones ofrecen recomendaciones concretas para México y la región iberoamericana, enfocadas en desarrollar capacidades propias, marcos regulatorios adecuados y esquemas de cooperación regional frente a un entorno estratégico cada vez más condicionado por la tecnología.

Palabras clave: Tecnologías de ruptura, seguridad nacional, inteligencia artificial, autonomía tecnológica, guerra en múltiples dominios.

Acerca de los autores: David Sánchez Hernández y Francisco Chávez Gutiérrez son investigadores del Instituto de Investigaciones Estratégicas de la Armada de México, adscrito al Centro de Estudios Superiores Navales de la Secretaría de Marina. Su trabajo se centra en el análisis estratégico, la seguridad nacional y el desarrollo tecnológico, combinando experiencia académica, profesional e investigativa para abordar problemáticas contemporáneas de interés institucional y nacional.

David Sánchez Hernández originario de Acapulco de Juárez, Guerrero es ingeniero industrial y de sistemas, con maestrías en Ingeniería de Sistemas y Sistemas Integrados de Gestión, además de un doctorado en Seguridad Pública. Actualmente cursa un segundo doctorado en Ciencias en Ingeniería Mecánica. Su formación incluye especializaciones en inteligencia para la seguridad nacional, análisis estratégico, gestión de sistemas y tecnologías aplicadas a la defensa. Ha desarrollado su carrera en el ámbito naval, académico e investigativo, con énfasis en seguridad pública, geopolítica, prospectiva estratégica, inteligencia y desarrollo de capacidades tecnológicas para la Secretaría de Marina.

Francisco Chávez Gutiérrez, originario de Suchiapa, Chiapas, es doctor en Ciencias de la Ingeniería por el TecNM/Instituto Tecnológico de Aguascalientes. Su trayectoria abarca la investigación y la formación de recursos humanos, con una maestría en Optomecatrónica por el Centro de Investigaciones en Óptica, A.C., donde ha trabajado en aplicaciones de metrología óptica, visión computacional y sistemas optomecatrónicos. Es ingeniero en Electrónica por el TecNM/Instituto Tecnológico de Tuxtla Gutiérrez, con experiencia en instrumentación y control.

La combinación de sus perfiles, uno con enfoque en seguridad y estrategia, el otro en ingeniería y desarrollo tecnológico, permite abordar los temas de investigación desde una perspectiva multidisciplinar. Esta sinergia enriquece el análisis de las tecnologías disruptivas y su influencia en la seguridad nacional, generando propuestas con mayor solidez y aplicabilidad.

Introducción

El orden internacional actual experimenta una transformación sin precedentes, impulsada por la rápida convergencia de tecnologías que rompen con los esquemas tradicionales. La cuarta revolución industrial, como la definió Schwab (2016), no se limita a la automatización o la digitalización; representa la fusión de lo físico, lo digital y lo biológico en un nuevo paradigma que trasciende las barreras sectoriales. En este escenario, la seguridad nacional, entendida como la protección de los intereses vitales de un Estado y su población, enfrenta desafíos de una complejidad inédita.

La tecnología siempre ha sido un factor clave en la competencia entre potencias. Pero hoy, su capacidad disruptiva¹, esa habilidad para alterar paradigmas de manera abrupta y acelerada, le otorga un peso estratégico único. Los Estados que logran dominar estas tecnologías emergentes adquieren ventajas que se traducen en poder militar, económico, informativo y político. Quienes no consiguen adaptarse, en cambio, quedan expuestos a riesgos como la marginalización, la dependencia o incluso vulnerabilidades directas en un contexto internacional cada vez más competitivo.

La expansión de la inteligencia artificial, la computación cuántica, los sistemas autónomos, la biotecnología y las tecnologías espaciales no solo está redefiniendo las operaciones militares del futuro, sino también el concepto mismo de soberanía. Como señalaba Nye (2011), el poder en el siglo XXI se vuelve "inteligente", combinando capacidades duras y blandas de formas que sitúan a la ventaja tecnológica en el centro de la ecuación. Hoy, infraestructuras críticas, sistemas financieros, redes de comunicación e incluso los procesos de toma de decisiones gubernamentales se han convertido en posibles escenarios de conflicto, aunque rara vez encajen en las definiciones clásicas de guerra.

Los conflictos ya no se parecen a lo que eran antes. Mary Kaldor lo planteó en 2012: las guerras modernas dejaron de ser asunto exclusivo de Estados para

¹ El término tecnología disruptiva fue popularizado por Clayton Christensen (1997) en *The Innovator's Dilemma* para referirse a innovaciones que transforman radicalmente mercados e industrias existentes. En el ámbito de la seguridad nacional, el concepto ha sido ampliado para incluir cualquier tecnología capaz de modificar de manera sustantiva el balance estratégico entre actores del sistema internacional.

convertirse en escenarios donde grupos armados sin bandera, redes que cruzan fronteras y herramientas tecnológicas recién estrenadas toman el protagonismo. Hoy esa tendencia no solo continúa, sino que se ha vuelto más compleja. Las llamadas guerras híbridas, los ataques cibernéticos sin autor reconocido, las campañas de desinformación que circulan como virus y el uso de sistemas autónomos que operan en silencio se han convertido en moneda corriente. Ya no hace falta declarar una guerra para librarla; basta con tener capacidad tecnológica y voluntad de usarla, ya sea desde un gobierno o desde un grupo que nadie sabe bien de dónde salió.

Lo que este trabajo intenta responder es cómo esas tecnologías que irrumpen sin aviso están cambiando las reglas de la seguridad nacional, la defensa y la competencia entre países. Más concretamente, qué significa todo esto para México y para los países de Iberoamérica. El propósito no es solo hacer un inventario, sino analizar las diez tecnologías que más están moviendo el tablero estratégico, entender qué riesgos traen consigo, qué oportunidades abren y qué escenarios podrían dibujarse hacia 2035.

La idea central aquí es clara: en el siglo XXI, la soberanía tecnológica², esa capacidad de un Estado para producir, adaptar, regular y proteger sus propias tecnologías críticas, ya no es un lujo, sino una condición básica para garantizar la seguridad nacional. El desafío no se reduce a comprar tecnología de última generación; de lo que se trata es de entenderla, gobernarla, integrarla en las instituciones y, sobre todo, desarrollar capacidades propias para no quedar atrapados en dependencias que, tarde o temprano, se convierten en vulnerabilidades estratégicas (FEM, 2023). Como señala el Foro Económico Mundial en su informe de 2023, el riesgo no está en la tecnología en sí, sino en la incapacidad de manejarla con autonomía.

El artículo sigue este recorrido: primero, analiza cómo la cuarta revolución industrial está redefiniendo el escenario estratégico global; después, examina en

² El concepto de soberanía tecnológica ha adquirido relevancia creciente en la política europea y latinoamericana como respuesta a la dependencia de infraestructuras digitales y cadenas de suministro de origen extranjero. Implica no solo la producción propia de tecnología, sino también la capacidad de regularla, protegerla y usarla de manera autónoma.

detalle esas diez tecnologías disruptivas que están reconfigurando la seguridad; luego, conecta estos análisis con los posibles escenarios operativos del futuro; a continuación, explora qué implicaciones tienen para la seguridad nacional en múltiples dimensiones; más adelante, identifica los riesgos estratégicos que están surgiendo; luego, pasa a las oportunidades que se abren; después, enfoca la mirada en México y en Iberoamérica; desarrolla tres escenarios prospectivos hacia 2035; y, por último, cierra con conclusiones y recomendaciones estratégicas.

Transformación tecnológica y cambio del entorno estratégico global

La cuarta revolución industrial no es solo otra etapa en la evolución tecnológica; marca un punto de quiebre en la forma en que entendemos el poder y las relaciones internacionales. A diferencia de las revoluciones anteriores, que avanzaban por sectores, primero la máquina de vapor, luego la electricidad, después la informática, esta vez el cambio no viene de una sola innovación, sino de la convergencia simultánea de varias. Inteligencia artificial (IA), robótica, *internet of Things* (IoT), computación en la nube, big data, biotecnología, nanotecnología, impresión 3D: todas estas tecnologías no solo evolucionan en paralelo, sino que se potencian entre sí. Klaus Schwab lo describió en 2016 como un fenómeno donde el todo es mucho más que la suma de las partes, y donde los efectos combinados generan dinámicas que ni los Estados ni sus instituciones de seguridad logran anticipar con claridad (Schwab, 2016).

Desde el punto de vista de la seguridad y la defensa, esta transformación tiene tres consecuencias estratégicas que vale la pena destacar. La primera es que el poder ya no se mide solo en términos tradicionales, territorio, población, recursos naturales o fuerza militar. Hoy, quien controla tecnologías clave como los semiconductores, la inteligencia artificial o las redes 5G adquiere una influencia que va más allá de su peso económico o militar. No se trata solo de tener armas más sofisticadas, sino de poseer las herramientas que definen las reglas del juego en el siglo XXI.

La segunda consecuencia es que el campo de batalla se ha expandido. Ya no se limita a tierra, mar y aire; ahora incluye el ciberespacio, el espacio exterior y lo que algunos llaman el dominio cognitivo-informacional. Esto significa que los

conflictos ya no se libran únicamente con tanques y aviones, sino también con ataques cibernéticos que paralizan infraestructuras críticas, campañas de desinformación que erosionan la confianza en las instituciones, sabotajes encubiertos a cadenas de suministro tecnológicas y operaciones que manipulan la percepción pública. La OTAN lo ha denominado competencia en el entorno multidominio, un concepto que refleja cómo las confrontaciones estratégicas han dejado de ser lineales para volverse difusas y multidimensionales (OTAN, 2022).

La tercera consecuencia es que el poder se está redistribuyendo de manera desigual. Estados Unidos y China lideran la carrera por el dominio en inteligencia artificial, semiconductores, computación cuántica y tecnologías espaciales, pero su rivalidad no es solo un asunto bilateral. Para los países con capacidades medias o emergentes, esta competencia entre gigantes presenta tanto riesgos como oportunidades. Por un lado, la dependencia tecnológica puede convertirse en una trampa; por otro, la búsqueda de autonomía estratégica abre caminos para posicionarse en el nuevo orden. Joseph Nye lo planteó en 2011: en un mundo donde la tecnología define el poder, los Estados que logren navegar entre estas tensiones tendrán más herramientas para defender sus intereses (Nye, 2011).

En este contexto, el concepto de "poder inteligente" que desarrolló Nye (2011) adquiere especial relevancia. Quienes logren dominar la producción de conocimiento tecnológico, establecer los estándares internacionales, gestionar las plataformas globales de datos y liderar la investigación en tecnologías de frontera concentrarán un tipo de poder que no se mide en misiles ni en tropas, pero que resulta decisivo para la seguridad y la influencia en el siglo XXI. La capacidad de actuar, o de impedir que otros actúen, en estos nuevos dominios estratégicos define, en gran medida, el perfil de seguridad de un Estado. Por eso, hoy la seguridad nacional ya no puede pensarse al margen de la política científica y tecnológica, ni de la capacidad institucional para gobernar estas tecnologías de manera soberana y responsable. Como señalaron Buzan y sus colaboradores en 1998, en un mundo interconectado, la seguridad ya no es solo un asunto militar, sino un desafío que atraviesa todas las dimensiones del Estado (Buzan *et al.*, 1998).

Principales tecnologías disruptivas con impacto en la seguridad nacional

Inteligencia artificial y aprendizaje automático

La inteligencia artificial y el aprendizaje automático son, sin duda, las tecnologías con mayor capacidad de transformación en el ámbito de la seguridad nacional. No se trata solo de máquinas que imitan comportamientos humanos, sino de sistemas capaces de reconocer patrones, procesar lenguaje natural, tomar decisiones, predecir escenarios y analizar imágenes con una precisión que, en muchos casos, supera a la humana. En el campo de la defensa y la seguridad, sus aplicaciones son tan amplias como variadas: desde el análisis masivo de datos de inteligencia hasta el desarrollo de sistemas de armas con altos niveles de autonomía en la toma de decisiones (OCDE, 2019).

Las ventajas que ofrece la IA para la seguridad nacional son considerables. En el ámbito de la inteligencia, permite procesar volúmenes de datos que antes resultaban inmanejables, integrando información de múltiples fuentes en tiempo real y reduciendo los plazos del ciclo de inteligencia. En ciberseguridad, los sistemas basados en IA detectan amenazas y anomalías con una rapidez y eficacia que los analistas humanos no pueden igualar. En el plano militar, optimiza la logística, mejora la planificación operativa y refuerza los sistemas de mando y control, facilitando la toma de decisiones en contextos complejos.

Pero los riesgos no son menores. El sesgo algorítmico, por ejemplo, puede generar discriminaciones sistemáticas en sistemas de vigilancia o en la gestión de amenazas, reproduciendo prejuicios que luego se traducen en políticas públicas o acciones militares. La opacidad de estos sistemas, ese problema de la “caja negra” que impide entender cómo llegan a sus conclusiones, plantea serias dudas sobre la responsabilidad jurídica y ética, especialmente cuando se trata de decisiones que pueden tener consecuencias letales. Además, la dependencia de grandes conjuntos de datos para entrenar estos sistemas los hace vulnerables a ataques de envenenamiento de datos o a manipulaciones adversariales, como señala un estudio de la RAND Corporation de 2020. La UNESCO (2021), ha insistido en la necesidad de establecer marcos éticos internacionales que regulen el desarrollo y el uso de la IA, sobre todo en sus aplicaciones militares.

Ciberseguridad, ciberdefensa y guerra cognitiva

Hoy nadie discute que el ciberespacio se ha convertido en el quinto escenario de confrontación militar y estratégica, al mismo nivel que los dominios tradicionales: tierra, mar, aire y espacio exterior. Lo que antes eran incidentes puntuales, ataques a redes eléctricas, sistemas de agua, hospitales, plataformas financieras o comunicaciones gubernamentales, se han normalizado como herramientas de presión, sabotaje y coerción entre Estados (Singer y Friedman, 2014). La publicación del *Tallinn Manual* (Schmitt, 2013) intentó, en su momento, adaptar el derecho internacional humanitario a este nuevo campo de batalla, pero su alcance sigue generando controversia entre los actores estatales.

La guerra cognitiva ha emergido como una de las formas más sutiles y peligrosas de conflicto actual. No se limita a vulnerar sistemas informáticos, sino que busca alterar percepciones, creencias y conductas de poblaciones enteras mediante campañas de desinformación, operaciones de influencia y manipulación del ecosistema informativo. La velocidad con la que circula la información en plataformas digitales complica su detección, atribución y neutralización oportuna (Castells, 2009).

En ciberseguridad, las oportunidades son claras: fortalecer capacidades nacionales para detectar y responder a incidentes, proteger infraestructuras críticas con arquitecturas de seguridad integradas desde el diseño, y fomentar la cooperación internacional en inteligencia sobre amenazas. Pero los riesgos no son menores. Herramientas de ciberataque de bajo costo están al alcance de actores no estatales, no existen normas internacionales vinculantes que regulen el ciberespacio, y atribuir responsabilidades con certeza suficiente para justificar represalias sigue siendo un desafío mayúsculo.

Drones, sistemas autónomos y plataformas no tripuladas

Los drones, o vehículos aéreos no tripulados (Unmanned Aerial Vehicles, UAV), han redefinido las operaciones militares y de vigilancia en los últimos diez años. Su expansión, tanto en el ámbito militar como civil y comercial, ha puesto al alcance de muchos lo que antes era privilegio de unas pocas potencias: capacidades de reconocimiento, vigilancia y acción remota. Su uso masivo en

conflictos recientes ha demostrado cómo estos sistemas pueden alterar el equilibrio táctico y operacional con un costo relativamente bajo.

Pero los sistemas no tripulados no se limitan al aire. Incluyen también vehículos marítimos de superficie y submarinos, así como plataformas terrestres autónomas. Esta diversificación ofrece ventajas clave: vigilancia continua, proyección de fuerza, apoyo logístico e incluso operaciones de minado, multiplicando la capacidad de combate de fuerzas convencionales (Scharre, 2018). Su despliegue en enjambres coordinados por inteligencia artificial plantea, además, un desafío estratégico para la defensa de infraestructuras y espacios aéreos nacionales.

En el ámbito civil y de seguridad pública, los drones tienen aplicaciones valiosas: vigilancia de fronteras, monitoreo de infraestructuras críticas, gestión de emergencias, combate al tráfico ilícito o patrullaje en zonas de difícil acceso. Sin embargo, también conllevan riesgos estratégicos. Pueden ser utilizados por organizaciones criminales, grupos terroristas o actores hostiles, la regulación internacional sigue siendo insuficiente, y su presencia en conflictos reduce el umbral político para el uso de la fuerza, generando nuevos dilemas de escalada.

Computación cuántica y criptografía poscuántica

La computación cuántica es, sin duda, uno de los avances tecnológicos con mayor potencial para revolucionar la seguridad de la información y, por extensión, la seguridad nacional. A diferencia de los sistemas clásicos, que operan con bits binarios, la computación cuántica utiliza qubits, capaces de mantener múltiples estados simultáneamente gracias al principio de superposición. Esto le otorga una capacidad de procesamiento exponencialmente superior para resolver problemas específicos, como la factorización de números enteros grandes, base de los sistemas de cifrado asimétrico más utilizados hoy.

El mayor peligro que plantea la computación cuántica para la seguridad nacional radica en su capacidad para vulnerar los sistemas criptográficos que protegen las comunicaciones digitales de gobiernos, ejércitos y sistemas financieros. Un actor con acceso a computadoras cuánticas lo suficientemente potentes podría descifrar comunicaciones encriptadas, comprometer sistemas de auten-

ticación y acceder a información clasificada de alto valor estratégico. Ante este escenario, el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha impulsado el desarrollo de estándares de criptografía poscuántica, diseñados para resistir este tipo de ataques.

Pero la computación cuántica no solo representa una amenaza. También abre oportunidades para la seguridad nacional: el desarrollo de sistemas de comunicación cuánticamente seguros, como las redes de distribución cuántica de claves, sensores de alta precisión con aplicaciones militares e de inteligencia, y simuladores para el diseño de nuevos materiales con usos estratégicos. La carrera por alcanzar la supremacía cuántica³ se ha convertido en uno de los ejes centrales de inversión en I+D de las principales potencias, con implicaciones estratégicas profundas para quienes logren desarrollar capacidades operativas primero.

Biotecnología, bioseguridad y riesgos epidemiológicos

La biotecnología de vanguardia, que incluye herramientas como *CRISPR-Cas9* para edición génica, biología sintética y diseño de organismos con características específicas, es un campo de doble uso con implicaciones directas para la seguridad nacional. Sus aplicaciones civiles son prometedoras: medicina de precisión, desarrollo de vacunas, mejora de cultivos o producción de biomateriales avanzados. Pero las mismas técnicas pueden ser empleadas para crear agentes biológicos con mayor virulencia, resistencia a tratamientos o capacidad de evadir el sistema inmunológico, lo que la convierte en un área crítica desde la perspectiva del control de armamentos.

La pandemia de COVID-19 dejó en evidencia la vulnerabilidad estratégica que representan las amenazas biológicas. Más allá del impacto sanitario, desencadenó crisis económicas, tensiones sociales, inestabilidad política y competen-

³ Se refiere al punto en que una computadora cuántica logra realizar una tarea computacional específica que una computadora clásica no podría resolver en un tiempo razonable. El concepto fue popularizado por John Preskill y cobró especial relevancia tras el experimento de Google con el procesador cuántico Sycamore, publicado en *Nature* en 2019, aunque su utilidad práctica y sus implicaciones operativas siguen siendo objeto de debate académico y tecnológico.

cia entre potencias por el acceso a vacunas, lo que se conoció como “diplomacia de vacunas”. Este episodio puso de manifiesto la necesidad de integrar la bioseguridad como un pilar fundamental en la planificación de seguridad nacional (Kaldor, 2012).

Gestionar los riesgos asociados al mal uso de la biotecnología es especialmente complejo. La mayoría del equipo y conocimiento en este campo tiene aplicaciones duales, los laboratorios privados con capacidades avanzadas se multiplican, verificar el cumplimiento de la Convención sobre Armas Biológicas y Tóxicas es difícil, y las tecnologías de edición génica están cada vez más al alcance de actores no estatales. Por ello, fortalecer capacidades nacionales en bioseguridad, con sistemas de alerta temprana, laboratorios de alta seguridad, marcos regulatorios robustos y cooperación internacional, se ha vuelto una prioridad estratégica ineludible.

Tecnologías espaciales, satélites y vigilancia estratégica

Lo que antes era un campo de estudio científico se ha convertido en un escenario clave para la estrategia global. Hoy, los satélites son piezas fundamentales en cualquier operación militar moderna: permiten la navegación precisa con sistemas GNSS, garantizan comunicaciones seguras, ofrecen inteligencia en tiempo real, alertan sobre lanzamientos de misiles y monitorean condiciones meteorológicas críticas. Pero esta dependencia también los convierte en objetivos prioritarios. Cualquier adversario con capacidad para interferirlos o destruirlos ganaría una ventaja decisiva, lo que obliga a repensar cómo proteger y hacer más resistentes estos activos en órbita.

El conflicto reciente en Ucrania dejó algo claro: los satélites comerciales en órbita baja ya no son un complemento, sino un factor que puede inclinar la balanza en una guerra convencional. Las constelaciones de comunicaciones que operan a baja altura han demostrado su valor al mantener la conectividad en zonas donde las infraestructuras tradicionales fallan, con consecuencias que van desde lo táctico hasta lo estratégico (SIPRI, 2023). El problema es que nadie anticipó del todo cómo estas capacidades privadas terminarían integrándose en las operaciones militares, dejando a los marcos regulatorios y doctrinales actuales un paso atrás.

La carrera por desarrollar armas antisatélite, desde misiles cinéticos hasta ciberataques, interferencias de señal o láseres de deslumbramiento, es uno de los frentes más preocupantes de la competencia estratégica actual. El Tratado del Espacio Exterior de 1967, que sigue siendo la base de la gobernanza espacial, no estaba diseñado para un escenario con estas amenazas ni con tantos actores nuevos. Para los países iberoamericanos, esto plantea un desafío doble: no solo necesitan acceso a datos satelitales y capacidad de lanzamiento, sino también voz en los foros donde se decide el futuro del espacio. Sin eso, la soberanía tecnológica queda en entredicho.

Robótica militar y sistemas autónomos letales

Los sistemas autónomos letales (LAWS, por sus siglas en inglés) están en el centro de uno de los debates más espinosos sobre el futuro de la guerra. A diferencia de las armas guiadas tradicionales, estos sistemas podrían identificar y atacar objetivos sin que un humano tome la decisión final en el momento crítico. Esto no solo complica la atribución de responsabilidades legales, sino que también obliga a replantearse cómo aplicar el derecho internacional humanitario y qué significa preservar la dignidad humana en un conflicto (Scharre, 2018).

Las discusiones en la Convención sobre Ciertas Armas Convencionales de la ONU han dejado al descubierto lo difícil que es llegar a un acuerdo sobre cómo regular, o incluso prohibir, estos sistemas. Algunos Estados se resisten a aceptar límites que puedan frenar sus programas de desarrollo militar, lo que abre la puerta a una carrera armamentista en autonomía que, una vez iniciada, sería casi imposible de detener. Para los países iberoamericanos, esto significa que no pueden quedarse al margen: necesitan definir posturas nacionales que encajen con sus marcos legales y estratégicos antes de que el debate los deje fuera de juego.

Pero más allá de las implicaciones éticas y jurídicas, la robótica militar ya está demostrando su utilidad en el terreno. Hay robots terrestres que evacúan heridos o desactivan minas, vehículos submarinos autónomos que vigilan puertos e infraestructuras críticas, drones que asumen misiones de alto riesgo y plataformas logísticas que reducen la exposición de los soldados en entornos

peligrosos. Entender estas capacidades, y sus límites, es clave para cualquier actor que quiera tener peso en las discusiones sobre el futuro de la guerra.

Big data, vigilancia digital y análisis predictivo

En el siglo XXI, los datos son el nuevo petróleo, pero con una diferencia crucial: su valor no está en extraerlos, sino en procesarlos. Quien logre recopilar, analizar y convertir en inteligencia grandes volúmenes de información tendrá una ventaja decisiva, ya sea en el mundo empresarial o en el de la seguridad nacional. Las agencias que dominan el big data pueden detectar patrones de comportamiento, anticipar movimientos de adversarios, identificar amenazas terroristas o criminales y respaldar decisiones estratégicas con una precisión y velocidad antes impensables (Castells, 2009). Y esto no se limita a fuentes cerradas: la combinación de datos abiertos, geolocalización, redes sociales y biométrica ha llevado la vigilancia estratégica a otro nivel.

El problema es que estos sistemas de vigilancia masiva, que incluyen reconocimiento facial, seguimiento de ubicaciones, análisis de redes sociales y monitoreo de comunicaciones, han reavivado un viejo debate: ¿hasta dónde puede llegar la seguridad sin sacrificar la privacidad? Pero hay otro riesgo menos visible: cuando los Estados dependen de plataformas tecnológicas extranjeras para almacenar y procesar estos datos, están entregando información sensible a jurisdicciones ajenas. Para países que no controlan su infraestructura digital, esto no es solo un tema de privacidad, sino de soberanía.

El análisis predictivo promete revolucionar la seguridad pública y la defensa, desde la prevención del crimen hasta el control de fronteras o la anticipación de conflictos. Sin embargo, su eficacia depende de algo que no siempre está garantizado: datos de calidad y modelos robustos. Si los sistemas de predicción del comportamiento criminal o de selección de objetivos militares están sesgados, el resultado puede ser desastroso, tanto para los derechos fundamentales como para la operatividad de las fuerzas de seguridad (Banco Mundial, 2021).

Semiconductores, cadenas de suministro críticas y dependencia tecnológica

Los semiconductores son el corazón invisible de casi toda la tecnología moderna: desde sistemas de armas hasta comunicaciones seguras, pasando por plataformas de inteligencia, infraestructuras críticas y hasta los dispositivos que usamos a diario. El problema es que su producción avanzada está concentrada en unas pocas fábricas en el mundo, lo que convierte a las cadenas de suministro globales en un punto débil estratégico (FEM, 2023). Esta vulnerabilidad ha convertido la política industrial tecnológica en un asunto de seguridad nacional.

La pugna entre Estados Unidos y China por dominar la cadena de suministro de semiconductores ha llevado a restricciones a la exportación, iniciativas para relocalizar la producción y alianzas tecnológicas con consecuencias geopolíticas profundas. Varios países han aprobado leyes para impulsar la fabricación local de chips y reducir su exposición a posibles interrupciones. Lo que antes era una cuestión de competitividad industrial ahora es parte central de la estrategia de seguridad nacional.

Para los países iberoamericanos, esta dependencia de semiconductores y otros componentes tecnológicos extranjeros es un talón de Aquiles. La región no tiene capacidad significativa para producir chips avanzados, lo que la deja expuesta a interrupciones en las cadenas de suministro y a presiones de las potencias tecnológicas. La solución no es sencilla, pero pasa por diversificar proveedores, fortalecer la industria de defensa local y explorar la cooperación regional. Si no se actúa, la vulnerabilidad seguirá creciendo.

Energías avanzadas, materiales estratégicos y tecnologías duales

El mundo está mirando hacia energías limpias y sistemas de almacenamiento más eficientes, pero ese cambio trae consigo un mapa distinto de dependencias estratégicas. Minerales como el litio, el cobalto o las tierras raras ya no son simples materias primas: son piezas clave en la fabricación de baterías, imanes para motores o componentes electrónicos avanzados. Quien controle su extracción y procesamiento tendrá una ventaja clara en la economía digital y en la industria de defensa. América Latina, con sus vastas reservas de litio y otros

minerales críticos, se encuentra en una posición privilegiada en este nuevo escenario energético global, algo que no pasa desapercibido en los análisis más recientes sobre el tema (CEPAL, 2022).

Hay tecnologías que sirven tanto para usos civiles como militares, y eso complica mucho las cosas cuando se trata de regular su exportación o evitar que caigan en manos equivocadas. Por ejemplo, la energía nuclear de cuarta generación, las baterías de estado sólido o los generadores de alta densidad energética pueden alimentar ciudades enteras o impulsar submarinos nucleares.

Tecnología	Oportunidades estratégicas	Riesgos principales	Aplicaciones de seguridad
Inteligencia artificial	Análisis de inteligencia, apoyo a C2, ciberseguridad proactiva, logística	Sesgo algorítmico, opacidad decisional, autonomía letal	Análisis predictivo, detección de amenazas, vigilancia
Ciberseguridad / guerra cognitiva	Protección de infraestructuras críticas, inteligencia de señales	Ataques a infraestructuras, desinformación masiva	Ciberdefensa nacional, operaciones de información
Drones y sistemas autónomos	Vigilancia persistente, ISR, operaciones en entornos hostiles	Proliferación, enjambres adversarios, umbral de escalada	Vigilancia fronteriza, reconocimiento, disuasión
Computación cuántica	Comunicaciones cuánticamente seguras, sensores de alta precisión	Ruptura del cifrado existente, asimetría tecnológica	Criptografía poscuántica, inteligencia de señales
Biotechnología	Vacunas, medicina de combate, detección CBRN	Armas biológicas, ingeniería de patógenos, biosabotaje	Detección CBRN, gestión sanitaria en emergencias
Tecnologías espaciales	ISR orbital, comunicaciones seguras, alerta temprana	Ataques antisatélite, fragmentación orbital, dependencia	Vigilancia estratégica, C2 en entornos degradados
Robótica militar / LAWS	Reducción del riesgo para combatientes, desminado, logística	Dilemas éticos y legales, LAWS, escalada no intencional	Operaciones en entornos contaminados o extremos
Big data y vigilancia	Análisis predictivo, inteligencia criminal, gestión de crisis	Vigilancia masiva, violación de privacidad, sesgo	Vigilancia fronteriza, prevención del delito, ISR
Semiconductores	Modernización de sistemas de defensa, soberanía tecnológica	Dependencia de proveedores externos, disrupciones de cadena	Sistemas embarcados, C2, armas guiadas de precisión
Energías y materiales críticos	Autonomía energética, ventaja en minerales estratégicos	Dependencia de importaciones, coerción económica	Propulsión naval, infraestructuras remotas, baterías tácticas

Tabla 1. Tecnologías disruptivas globales: oportunidades, riesgos y aplicaciones de seguridad nacional. Nota. Elaboración propia a partir de datos de OCDE (2019), Scharre (2018), FEM (2023) y SIPRI (2023).

Gestionar esa dualidad exige marcos regulatorios complejos y equipos de inteligencia especializados, algo que en Iberoamérica aún está en construcción. La mayoría de los países de la región están dando sus primeros pasos en este terreno, tratando de cerrar la brecha entre sus capacidades actuales y lo que realmente necesitan.

Tecnologías disruptivas y el futuro de las operaciones militares

Las guerras del futuro no se parecerán en nada a las del pasado. El concepto de operaciones multidominio, o Multi-Domain Operations (MDO), como lo llaman en la doctrina anglosajona, propone que los ejércitos ya no pueden actuar de forma aislada en tierra, mar o aire. Ahora deben operar de manera coordinada en seis frentes: terrestre, naval, aéreo, espacial, cibernético e incluso en el ámbito cognitivo-informacional. Este enfoque rompe con la segmentación tradicional de las doctrinas del siglo XX y exige cambios profundos en la forma en que los ejércitos se organizan, se entrenan y adquieren tecnología. Para los países de la región, el mensaje es claro: no hay tiempo que perder (OTAN, 2022).

Lo que antes tomaba horas o días ahora se decidirá en minutos o segundos. La inteligencia artificial aplicada al ciclo de inteligencia y al mando y control está acelerando los procesos de decisión a un ritmo que los humanos difícilmente pueden seguir. El modelo OODA (Observar, Orientar, Decidir, Actuar) se comprime hasta límites insospechados gracias a sensores autónomos y algoritmos capaces de procesar información en tiempo real. Quien logre imponer su ritmo en este nuevo entorno tendrá una ventaja táctica decisiva. Pero esta "velocidad de máquina" plantea preguntas incómodas: ¿qué papel le queda al juicio humano en la toma de decisiones letales? ¿Cómo se supervisa y se rinde cuentas cuando las acciones ocurren a una escala de tiempo que escapa al control directo de las personas?

En los campos de batalla del futuro, las fuerzas militares operarán con una mezcla de plataformas tripuladas y no tripuladas, capaces de actuar en entornos hostiles donde el acceso es limitado o está en disputa. La guerra electrónica, las interferencias en el espectro electromagnético y los ciberataques contra sistemas de navegación y comunicaciones obligarán a los ejércitos a ser más resilientes. La dependencia de datos en tiempo real, aunque ofrece ventajas

tácticas evidentes, también abre nuevas vulnerabilidades. Los adversarios no dudarán en explotarlas, convirtiendo la información en un arma tan poderosa como cualquier proyectil.

La información será tan determinante como la fuerza bruta. Las operaciones de influencia, la desinformación estratégica y la manipulación del espacio cognitivo, tanto de la población como de las élites políticas, se utilizarán antes, durante y después de cualquier conflicto convencional. Esta convergencia entre lo informacional y lo militar exige que los Estados desarrollen doctrinas integradas y estructuras capaces de responder de manera coordinada en todos los frentes. Ya no basta con tener un ejército bien equipado; también hay que saber manejar el relato, anticipar las narrativas del adversario y proteger la percepción pública de la realidad.

Para los países iberoamericanos, adaptarse a esta transformación no significa necesariamente adquirir las tecnologías más avanzadas del mercado. En muchos casos, integrar de manera inteligente las capacidades existentes, a través de arquitecturas abiertas e interoperables, puede generar ventajas operativas significativas sin requerir inversiones desproporcionadas. Lo verdaderamente crítico no es tener los sistemas más modernos, sino entender cómo encajan entre sí y contar con instituciones capaces de gestionar esa integración. La tecnología, al final, es solo una herramienta; lo que marca la diferencia es cómo se usa.

Implicaciones para la seguridad nacional

Las tecnologías disruptivas no afectan solo a un área de la seguridad nacional, sino a todas. Si tomamos el marco de Buzan (1998), que divide la seguridad en sectores interconectados, podemos ver cómo la transformación tecnológica impacta en cada uno de ellos: político, económico, social, militar, tecnológico, diplomático y ambiental. Cada dimensión presenta sus propias oportunidades y riesgos, y los Estados deben abordarlos de manera integral si quieren evitar desequilibrios peligrosos.

Dimensión política

En el ámbito político, la tecnología está redefiniendo las reglas del juego. La velocidad con la que fluye la información digital y la capacidad de las redes sociales para movilizar a la sociedad en tiempo real han dejado obsoletos muchos mecanismos tradicionales de gobernanza. Las herramientas de vigilancia avanzada pueden ser un arma de doble filo: en regímenes autoritarios, refuerzan el control social; en democracias, chocan con los derechos a la privacidad y la libertad de expresión. Regular a las grandes plataformas tecnológicas y definir qué significa realmente la soberanía digital ya no son debates teóricos, sino cuestiones de seguridad nacional que exigen respuestas urgentes.

Dimensión económica

La competencia tecnológica está reconfigurando el poder económico. La capacidad de un país para innovar y producir tecnologías críticas determina su competitividad industrial, la resiliencia de sus cadenas de suministro y su capacidad para financiar su defensa. Depender de proveedores externos en áreas estratégicas es un riesgo que puede materializarse en forma de sanciones, restricciones de exportación o presiones políticas. Por eso, desarrollar una base industrial de defensa propia no es un gasto, sino una inversión en autonomía estratégica y soberanía tecnológica. Y como toda inversión a largo plazo, requiere visión, paciencia y recursos (FEM, 2023).

La dimensión social

Las tecnologías que irrumpen en nuestra realidad no solo transforman procesos, sino que reconfiguran los vínculos entre las personas. Por un lado, abren puertas a formas inéditas de conexión: permiten que comunidades dispersas se organicen, que voces marginadas encuentren eco y que la ciudadanía exija mayor transparencia a sus gobiernos. Pero esa misma capacidad de difusión masiva se convierte en un arma cuando se usa para propagar mentiras o discursos que siembran odio. La desconfianza hacia las instituciones no surge de la nada; se alimenta de narrativas que distorsionan la realidad y polarizan a la sociedad hasta fracturarla. El problema se agrava cuando el acceso a estas tecnologías no es equitativo. Quienes quedan al margen, por falta de recursos,

educación o infraestructura, ven cómo la brecha con los demás no solo persiste, sino que se ensancha. No se trata solo de quedarse atrás en oportunidades económicas; es quedar excluido de espacios donde se toman decisiones que afectan a todos. Y cuando la desigualdad tecnológica se superpone a otras formas de exclusión, el riesgo de inestabilidad social se multiplica. Eso sí, no todo es amenaza: herramientas como las plataformas de participación ciudadana o los sistemas de gobierno abierto demuestran que, bien usadas, estas tecnologías pueden ser un puente hacia sociedades más cohesionadas (Castells, 2009).

La dimensión militar

Hoy, la capacidad de un ejército para cumplir su misión depende, en gran medida, de algo que va más allá de los soldados o el armamento tradicional. La tecnología se ha convertido en el factor que inclina la balanza en un escenario estratégico cada vez más complejo. No basta con modernizar equipos; hay que repensar cómo se integran sistemas autónomos, inteligencia artificial o capacidades cibernéticas en las doctrinas existentes. Esto exige inversiones continuas: no solo en hardware, sino en formación para quienes operarán estas herramientas y en marcos conceptuales que las hagan efectivas. Pero la disuasión ya no se limita a mostrar músculo con tanques o aviones. Ahora, lo que cuenta es la percepción que tengan los adversarios sobre las capacidades tecnológicas propias. Si un país logra transmitir que sus sistemas son lo suficientemente avanzados como para neutralizar cualquier ventaja que otro pudiera obtener en un ataque, la disuasión cumple su objetivo. El problema es que, en este juego de percepciones, un error de cálculo o una brecha tecnológica no detectada a tiempo pueden tener consecuencias impredecibles.

La dimensión tecnológica

En el siglo XXI, la seguridad nacional ya no se mide solo por la fortaleza de las fronteras o el tamaño de las fuerzas armadas. Lo que define la autonomía de un Estado es su capacidad para controlar, o al menos no depender críticamente de otros, las tecnologías que sustentan su funcionamiento. Esto implica producir lo esencial dentro de sus propias fronteras, proteger su infraestructura digital de intrusiones, regular el uso de estas herramientas en su territorio y, sobre todo, tener voz en la mesa donde se deciden las reglas del juego global. Los

países que no logran este nivel de autonomía quedan atrapados en una relación de dependencia peligrosa. No se trata solo de comprar tecnología a proveedores extranjeros; es someterse a sus prioridades, a sus decisiones comerciales e incluso a posibles vulnerabilidades ocultas en el hardware o software que adquieren. Y cuando los intereses de esos actores externos chocan con los propios, los instrumentos tradicionales de seguridad nacional, como la diplomacia o la defensa, resultan insuficientes para protegerse.

La dimensión diplomática

La competencia tecnológica está reescribiendo el mapa de las alianzas internacionales. Hoy, países que comparten visiones sobre inteligencia artificial, ciberseguridad o comunicaciones seguras se agrupan en iniciativas que, en muchos casos, terminan por redefinir sus relaciones de seguridad tradicionales. Para Iberoamérica, participar activamente en estos foros no es un lujo, sino una necesidad. Si un país no está presente en los espacios donde se discuten las normas que regirán el uso de estas tecnologías, está aceptando, de facto, que otros decidan por él (Naciones Unidas, 2021). La ausencia en estos debates no es neutral: equivale a renunciar a moldear el entorno normativo que, tarde o temprano, afectará a todos. Y en un mundo donde la tecnología avanza más rápido que la capacidad de los Estados para regularla, quedarse al margen puede significar perder la oportunidad de influir en cuestiones que van desde la privacidad de los datos hasta los límites éticos de la automatización en conflictos armados.

La dimensión ambiental

Las tecnologías disruptivas no solo transforman industrias o sociedades; también ofrecen herramientas clave para enfrentar uno de los mayores desafíos del siglo: la crisis ambiental. Satélites que monitorean el clima, sistemas de análisis de datos que predicen desastres naturales o redes de sensores distribuidos en territorios remotos permiten vigilar ecosistemas y fronteras con una precisión impensable hace unas décadas. Estas capacidades no solo sirven para proteger recursos naturales; también son fundamentales para la seguridad humana, desde la gestión de emergencias hasta la defensa de territorios estratégicos. Pero hay un lado oscuro. La producción de estas tecnologías, es-

pecialmente semiconductores, baterías o componentes electrónicos, deja una huella ambiental profunda. La extracción de minerales raros, los procesos industriales contaminantes y los residuos generados plantean dilemas éticos y prácticos. ¿Cómo conciliar la necesidad de avanzar tecnológicamente con los compromisos de sostenibilidad que los Estados han asumido? La respuesta no está en frenar el progreso, sino en diseñar marcos regulatorios que obliguen a las empresas a internalizar los costos ambientales de sus actividades.

Riesgos estratégicos emergentes

El ritmo acelerado de la innovación tecnológica no solo trae oportunidades; también abre una caja de Pandora de riesgos que los Estados deben gestionar con urgencia. El más evidente es la dependencia externa. Cuando un país no desarrolla capacidades propias en tecnologías críticas, queda a merced de sus proveedores. No se trata solo de que estos puedan cortar el suministro por razones comerciales o políticas; es que podrían introducir vulnerabilidades deliberadas en el hardware o software que exportan, dejando al país expuesto a ciberataques o sabotajes. Esta dependencia no es un problema teórico. Ya hemos visto cómo decisiones unilaterales de empresas o gobiernos extranjeros pueden paralizar sectores enteros de un país en cuestión de horas. Y lo peor es que, en muchos casos, los instrumentos tradicionales de seguridad nacional, como la diplomacia o la disuasión militar, resultan ineficaces para contrarrestar estas amenazas.

Otro riesgo que no puede ignorarse es la vulnerabilidad de las infraestructuras críticas. Redes eléctricas, acueductos, oleoductos, sistemas de salud o comunicaciones gubernamentales son cada vez más digitales y, por tanto, más expuestos a ciberataques. Un solo fallo en estos sistemas puede desencadenar efectos en cascada: desde cortes de energía prolongados hasta el colapso de servicios esenciales. Y lo más preocupante es que, a diferencia de un ataque armado convencional, un ciberataque exitoso no siempre deja huellas claras. Esto plantea un dilema jurídico y político: ¿cómo responder a una agresión que no sigue las reglas tradicionales de la guerra? Los marcos legales actuales no están preparados para este escenario, y la falta de consenso internacional sobre qué constituye un acto de guerra en el ciberespacio solo agrava el problema.

El poder concentrado en unas pocas corporaciones tecnológicas, las llamadas hiperescalares, representa otro desafío sin precedentes. Empresas con valoraciones de mercado superiores al PIB de muchos países controlan infraestructuras digitales críticas, plataformas de comunicación masiva y volúmenes de datos que las convierten en actores clave del sistema internacional. Esta concentración de poder crea asimetrías peligrosas: los Estados, incluso los más poderosos, a menudo carecen de herramientas para regular efectivamente a estas corporaciones. Los marcos legales existentes, tanto nacionales como internacionales, fueron diseñados para un mundo donde el poder se medía en términos militares o económicos tradicionales. Hoy, sin embargo, una sola empresa puede decidir el destino de millones de personas con solo cambiar sus algoritmos o políticas de privacidad. Y lo más preocupante es que, en muchos casos, estas decisiones se toman sin transparencia y sin rendición de cuentas.

La desinformación y la guerra cognitiva son, quizás, los riesgos más insidiosos de la era digital. Actores hostiles, ya sean Estados o grupos no estatales, pueden difundir narrativas falsas o manipuladoras a escala masiva, con costos mínimos y alta capacidad de negación. El problema no es solo que estas campañas distorsionen la realidad; es que erosionan la confianza en las instituciones, polarizan a la sociedad y, en casos extremos, pueden desencadenar conflictos. Las herramientas para generar contenido sintético, como los *deepfakes*, han llevado esta amenaza a otro nivel. Hoy, es posible crear videos o audios falsos tan convincentes que resulta casi imposible distinguirlos de la realidad. Y aunque los avances en detección de falsificaciones avanzan, la velocidad a la que se propagan estos contenidos en redes sociales hace que el daño ya esté hecho antes de que alguien pueda desmentirlos.

La carrera armamentista tecnológica entre las grandes potencias añade otro nivel de riesgo: el de un conflicto accidental o una escalada no intencional. Cuando los sistemas de alerta temprana y toma de decisiones incorporan inteligencia artificial, cualquier error, un falso positivo, una interpretación equivocada de los datos, puede desencadenar una respuesta automática con consecuencias catastróficas. La pérdida de control humano sobre estos sistemas en situaciones de alta tensión es uno de los escenarios que más preocupa a los analistas. Imaginemos un algoritmo que, ante una amenaza percibida, active protocolos de defensa sin que medie intervención humana. En un contexto de desconfianza mutua entre potencias, este tipo de errores podría llevar a una

escalada que nadie desea, pero que nadie podría detener a tiempo. La comunidad internacional ha comenzado a discutir estos riesgos, pero el ritmo de la innovación tecnológica supera con creces la capacidad de los Estados para regularla (RAND Corporation, 2020).

La brecha tecnológica entre países con capacidades avanzadas y aquellos que van a la zaga no solo pone en riesgo a estos últimos, sino que termina por debilitar la estabilidad del sistema internacional. Los Estados que no logran desarrollar infraestructuras básicas en ciberseguridad, gestión de datos o conectividad digital se convierten en puntos vulnerables dentro de redes globales. Su fragilidad los expone a convertirse en canales involuntarios de amenazas para sus vecinos, además de quedar a merced de actores externos que explotan esa dependencia para imponer presiones políticas o económicas.

Oportunidades estratégicas para los Estados

Ante estos riesgos, las tecnologías disruptivas abren un abanico de posibilidades para que los Estados refuercen su seguridad nacional, siempre que se gestionen con una perspectiva de largo plazo y con instituciones sólidas. En el ámbito de la inteligencia, por ejemplo, la combinación de fuentes abiertas digitales, el monitoreo de redes sociales, herramientas de geolocalización y análisis predictivo con inteligencia artificial permite construir una imagen más precisa y oportuna de los escenarios estratégicos. Esto no solo mejora la capacidad de anticipación ante crisis, sino que facilita una respuesta más ágil cuando estas se materializan.

En el terreno de la seguridad pública, las tecnologías ofrecen herramientas valiosas para enfrentar amenazas transnacionales. Sistemas de vigilancia inteligente, análisis forense digital, interceptación de comunicaciones de grupos criminales y el mapeo de redes del crimen organizado han demostrado ser eficaces contra el narcotráfico, el terrorismo o el tráfico de personas. El análisis de grandes volúmenes de datos financieros, por su parte, puede revelar patrones de lavado de dinero y desarticular las estructuras económicas que sostienen estas actividades. Eso sí, su efectividad depende de que existan marcos legales claros que garanticen su uso dentro de los límites del Estado de derecho, sin menoscabar los derechos fundamentales.

Para la defensa del territorio y los recursos naturales, la tecnología también representa una ventaja estratégica. Satélites de observación, sistemas de vigilancia marítima con drones y sensores remotos distribuidos permiten cubrir extensiones vastas de mar territorial, zonas económicas exclusivas o fronteras terrestres que, con métodos convencionales, serían inabarcables. En el caso de los países iberoamericanos, con territorios marítimos y terrestres extensos, estas soluciones tecnológicas ofrecen una forma relativamente económica de mejorar su conciencia situacional estratégica de manera significativa.

Invertir en investigación científica y tecnológica básica, en universidades y centros de excelencia, puede generar capacidades nacionales autónomas en áreas estratégicas. Formar profesionales especializados en inteligencia artificial, ciberseguridad, biotecnología o computación avanzada no es un gasto, sino una inversión a largo plazo. El talento humano, no solo la infraestructura, es el factor decisivo para construir una soberanía tecnológica que perdure. Los Estados deben diseñar políticas educativas y de ciencia y tecnología alineadas con sus objetivos de seguridad nacional si quieren evitar dependencias externas.

Perspectiva para México e Iberoamérica

México e Iberoamérica enfrentan la transformación tecnológica desde una posición particularmente vulnerable. Por un lado, la distancia con las grandes potencias en materia tecnológica es considerable y, sin políticas activas de inversión y cooperación, tiende a ensancharse. Por otro, la creciente digitalización de sus economías e instituciones públicas las expone cada vez más a ciberamenazas, desinformación y dependencias tecnológicas, sin que hayan desarrollado las capacidades necesarias para responder con eficacia. Esta combinación de exposición creciente y respuestas insuficientes configura un desafío estratégico que exige atención inmediata.

A pesar de estos retos, la región cuenta con activos estratégicos que, bien gestionados, podrían marcar la diferencia. América Latina alberga reservas significativas de litio, cobre, cobalto, niobio y tierras raras, materiales esenciales para la economía digital y la industria de defensa global. Si estos recursos se gestionan con soberanía, incorporando procesos de valor agregado a nivel na-

cional, con marcos regulatorios justos y estrategias de negociación multilateral, podrían traducirse en capacidad tecnológica e influencia estratégica. La CEPAL (2022) ha insistido en la necesidad de vincular la transición energética con el desarrollo industrial y la autonomía estratégica regional (CEPAL, 2022).

En ciberseguridad, sin embargo, el panorama regional es preocupante. La mayoría de los países iberoamericanos no tienen estrategias nacionales actualizadas, legislación especializada robusta, equipos de respuesta a incidentes con capacidades adecuadas ni suficiente personal especializado. Formar profesionales en ciberseguridad, inteligencia de amenazas y gestión de incidentes debe ser una prioridad, y requiere coordinación entre ministerios de defensa, seguridad, educación y telecomunicaciones, así como una colaboración estrecha con la academia y el sector privado.

La cooperación regional en seguridad tecnológica podría ser la clave para superar las limitaciones individuales de cada país. Los mecanismos de cooperación en defensa e inteligencia que ya existen en la región podrían ampliarse para incluir la dimensión cibernética, la protección de infraestructuras críticas, el intercambio de inteligencia sobre amenazas tecnológicas y la coordinación de posturas en foros internacionales de gobernanza tecnológica. En este sentido, la ACDIA, como plataforma de formación y diálogo estratégico entre los centros superiores de defensa iberoamericanos, podría jugar un papel relevante en la construcción de esta agenda.

México, en particular, tiene condiciones para posicionarse como un actor clave en la gobernanza regional de tecnologías de seguridad. Su ubicación geográfica, el tamaño de su economía, su capital humano en ciencia y tecnología, y sus vínculos con los principales actores tecnológicos globales le dan una base desde la cual podría liderar iniciativas regionales en ciberseguridad, bioseguridad y gobernanza de la inteligencia artificial. El Programa para la Seguridad Nacional 2020-2024 (Gobierno de México, 2020) reconoce la importancia de estas amenazas emergentes, aunque la implementación de políticas concretas sigue siendo un desafío que demanda recursos, voluntad política y una coordinación institucional sostenida.

También es urgente modernizar los centros de estudios superiores de defensa en la región para incorporar, de manera sistemática, la enseñanza de tecnologías disruptivas, ciberseguridad, análisis estratégico en entornos multidominio

e inteligencia artificial. Formar a las élites militares y civiles de defensa en estos ámbitos no es solo una necesidad operativa, sino una condición para que los países iberoamericanos puedan participar con voz propia en los debates internacionales sobre la gobernanza de las tecnologías militares emergentes.

Escenarios prospectivos

Escenario tendencial: adaptación desigual hacia 2035

En este escenario, los Estados adoptan las tecnologías disruptivas de manera gradual y desigual, avanzando en función de sus capacidades económicas, institucionales y de capital humano. Las grandes potencias consolidan su liderazgo en inteligencia artificial, computación cuántica y tecnologías espaciales, mientras que los países de capacidades medias y emergentes progresan de forma incremental en la digitalización de sus sistemas de seguridad y defensa, casi siempre mediante la adopción de tecnologías desarrolladas por terceros. La dependencia tecnológica externa sigue siendo una constante para la mayoría de los países iberoamericanos, con esfuerzos aislados de diversificación y desarrollo de capacidades propias que no logran alterar de manera significativa la asimetría existente. La cooperación internacional en gobernanza tecnológica avanza a paso lento, con acuerdos parciales en áreas específicas, pero sin marcos normativos globales vinculantes y comprehensivos.

Escenarios de riesgo: escalada tecnológica y fragmentación hacia 2035

Para 2035, la carrera tecnológica entre potencias no se limita a quién llega primero, sino a quién controla el tablero. El resultado es una internet fracturada, la llamada splinternet, donde cada bloque impone sus propias reglas, sus estándares incompatibles, sus fronteras digitales. Los ciberataques contra centrales eléctricas, hospitales o redes financieras dejan de ser incidentes aislados para convertirse en actos con consecuencias diplomáticas, incluso militares. Sistemas autónomos capaces de decidir sobre vida o muerte operan sin supervisión efectiva, y un error de cálculo podría desencadenar una escalada que nadie buscó. Mientras tanto, la desinformación se vuelve sistemática: socava la confianza en las instituciones, polariza sociedades y debilita democra-

cias enteras. Los países iberoamericanos, con capacidades tecnológicas limitadas, quedan atrapados en una dependencia peligrosa. Proveedores externos condicionan el acceso a tecnologías esenciales, imponiendo no solo costos económicos, sino también exigencias políticas que erosionan su autonomía estratégica y su capacidad de defensa.

Escenario ideal: soberanía tecnología y gobernanza responsable hacia 2035

En el mejor de los casos, los Estados logran algo que hoy parece lejano: dominar las tecnologías críticas sin depender de terceros. No se trata solo de producir semiconductores o desarrollar inteligencia artificial, sino de regular su uso, protegerse de sus riesgos y cooperar para que su impacto sea positivo. Iberoamérica, en particular, avanza hacia una plataforma regional de ciberseguridad, donde los países comparten inteligencia, capacitan a sus expertos y responden de manera coordinada a las amenazas. Se firman acuerdos internacionales vinculantes sobre armas autónomas y comportamiento en el ciberespacio, con participación activa de la región en su diseño. La inversión en ciencia y tecnología deja de ser un gasto para convertirse en una apuesta estratégica: se desarrollan capacidades propias en biotecnología, energía avanzada y microelectrónica, reduciendo la dependencia externa y fortaleciendo tanto la industria de defensa como la autonomía nacional.

Conclusión

El recorrido anterior permite extraer algunas certezas incómodas, pero necesarias. La primera es que la tecnología ya no es un simple complemento de la seguridad nacional. Hoy define el poder de los Estados, su soberanía y su capacidad para protegerse. La competencia tecnológica no es un capítulo aparte de la geopolítica: es uno de sus ejes centrales, tan determinante como el equilibrio militar tradicional. Quien ignore esto, quedará relegado en un mundo donde las reglas las escriben quienes dominan la innovación.

La segunda certeza es que la soberanía tecnológica no es un lujo, sino una condición básica para la supervivencia en el siglo XXI. Los países que dependen

de infraestructuras, plataformas o tecnologías extranjeras están expuestos a formas de coerción que los mecanismos de seguridad tradicionales no pueden contrarrestar. No se trata solo de comprar equipos, sino de desarrollar capacidades propias: investigar, adaptar, regular y proteger. Fortalecer la base científica e industrial no es un tema de desarrollo económico, sino una cuestión de seguridad nacional.

La tercera es que los conflictos del futuro no se parecerán a los del pasado. Las operaciones ya no se limitan a tierra, mar o aire; ahora abarcan el ciberespacio, el dominio cognitivo y la inteligencia artificial. La velocidad de decisión, la integración de sistemas tripulados y no tripulados, y la guerra de narrativas exigen una revisión profunda de las doctrinas militares. Quienes se aferren a los paradigmas del siglo XX verán cómo su capacidad de disuasión se debilita, mientras el mundo avanza hacia un escenario donde la tecnología marca el ritmo de la estrategia.

La cuarta es que el desafío no es solo técnico o militar. Requiere instituciones sólidas en lo jurídico, lo político y lo educativo. Los marcos regulatorios deben evolucionar para abordar conflictos híbridos, el impacto de los sistemas autónomos en los derechos humanos y el uso de datos en contextos de seguridad. México e Iberoamérica no pueden quedarse al margen de estos debates. Su participación en la gobernanza tecnológica global no es opcional: es una necesidad estratégica, y cada día de retraso aumenta los costos y reduce las opciones.

Recomendación estratégica

Hoy, la seguridad nacional ya no se defiende solo con tanques, barcos o aviones. Se juega en los cables submarinos que conectan continentes, en los centros de datos que almacenan información crítica, en los laboratorios donde se diseña el futuro. Los minerales estratégicos, los algoritmos, los satélites: todo forma parte de un tablero donde el poder se mide en capacidad tecnológica. Quien no lo entienda a tiempo, llegará tarde a una guerra que no tendrá declaración formal, pero cuyas consecuencias serán igual de reales.

Para México y los países iberoamericanos, esto no es un llamado a comprar más tecnología, sino a repensar su enfoque. No basta con modernizar equipos si las estructuras, las doctrinas y la cultura institucional siguen ancladas en el pasado. La transformación debe ser profunda: en cómo se planifica la defensa, en cómo se forma a los líderes, en cómo se protegen las infraestructuras críticas.

Lo primero es integrar la dimensión tecnológica en el corazón de las estrategias de seguridad. La ciberseguridad, la bioseguridad, la inteligencia estratégica y la soberanía tecnológica no pueden seguir siendo temas secundarios, relegados a informes técnicos o reuniones de especialistas. Deben ocupar un lugar central en la agenda del Estado, con objetivos claros, plazos definidos y recursos suficientes. Sin evaluaciones periódicas, hasta la estrategia más elaborada termina convertida en un documento bonito, pero inútil cuando llega la crisis.

En el ámbito militar, las doctrinas deben actualizarse para reflejar la realidad de las operaciones multidominio. El campo de batalla ya no respeta divisiones limpias entre tierra, aire, mar o ciberespacio. Un ataque digital puede paralizar una ciudad; una campaña de desinformación, desestabilizar un gobierno; un sistema autónomo, cambiar el curso de una batalla en segundos. La defensa del siglo XXI exige entender que todo está conectado, y que la seguridad ya no se limita a proteger fronteras físicas.

Los centros de formación militar tienen aquí un papel clave. Sus programas deben incorporar tecnologías emergentes, inteligencia artificial aplicada a la seguridad y análisis estratégico en entornos digitalizados. Formar líderes con manuales del siglo XX es como enseñar a navegar con un mapa de caminos rurales: puede tener cierto encanto, pero es insuficiente para enfrentar los desafíos actuales.

La ciberseguridad, en particular, requiere atención prioritaria. México y los países iberoamericanos deben fortalecer sus Equipos Nacionales de Respuesta a Incidentes Cibernéticos, actualizar sus marcos legales y proteger las infraestructuras críticas. Energía, telecomunicaciones, finanzas, transporte, salud: todos estos sectores dependen de sistemas vulnerables a ataques que no requieren cruzar fronteras, sino solo explotar una vulnerabilidad. El enemigo ya no necesita invadir un territorio; le basta con encontrar una contraseña débil o un eslabón descuidado en la cadena.

La ciberseguridad no puede seguir siendo un tema secundario en la agenda nacional. Las becas, los convenios con universidades, los centros de investigación avanzada y la colaboración con el sector tecnológico no son gastos superfluos, sino apuestas necesarias. Aquí, el factor humano marca la diferencia tanto como la infraestructura. Un país sin profesionales propios termina atado a soluciones externas, y esa dependencia, por más que se disfraze con contratos de última generación, sigue siendo eso: dependencia.

La soberanía tecnológica plantea otro reto fundamental. Los países iberoamericanos necesitan impulsar políticas industriales que, al menos de manera coordinada y parcial, permitan producir componentes críticos, desarrollar software seguro para áreas gubernamentales sensibles y construir plataformas de comunicación confiables. No se trata de perseguir utopías autárquicas ni de levantar barreras digitales imposibles, sino de reducir riesgos estratégicos. En este ámbito, la soberanía no significa hacer todo en solitario, sino evitar quedar a merced de decisiones ajenas.

En este contexto, los minerales estratégicos ganan un peso geopolítico cada vez mayor. El litio, las tierras raras y otros insumos clave para baterías, electrónica, energías limpias y tecnologías avanzadas no debe gestionarse únicamente como material primas de exportación. América Latina ya vivió esta historia: extraer riqueza del suelo para ver cómo otros la transforman en valor agregado. La distancia entre vender materias primas y desarrollar capacidades industriales es la misma que hay entre ser proveedor y ser diseñador.

Por eso, la gestión de estos recursos debe ir de la mano con políticas de industrialización, innovación, transferencia tecnológica y colaboración regional. El beneficio no puede quedarse en ingresos fiscales inmediatos. Tiene que traducirse en conocimiento, empleo especializado, infraestructura productiva y autonomía estratégica real.

La cooperación iberoamericana no es un adorno, sino una necesidad urgente. Ningún país de la región, por sí solo, está en condiciones de enfrentar con eficacia los desafíos que plantean la inteligencia artificial, la guerra cognitiva, la bioseguridad, los ciberataques transfronterizos o la protección de infraestructuras críticas. La fragmentación regional puede sonar bien en discursos soberanistas, pero es un lujo que la seguridad tecnológica no puede permitirse. En

un mundo donde las potencias operan a escala continental, actuar como islas dispersas es, en el fondo, una forma elegante de condenarse a la irrelevancia.

Por ello, sería conveniente promover mecanismos específicos de cooperación iberoamericana en áreas como ciberseguridad, gobernanza de la inteligencia artificial, bioseguridad y protección de infraestructuras críticas. Espacios académicos y de formación, como la Asociación de Colegios de Defensa Iberoamericanos, podrían servir de puente para crear una comunidad regional de conocimiento estratégico. Una red capaz de generar doctrina propia, intercambiar experiencias, formar especialistas e incidir con voz propia en los debates globales sobre tecnologías militares emergentes.

La región no parte de cero. Cuenta con universidades, fuerzas armadas profesionales, recursos naturales, talento joven, tradición diplomática y una ubicación geopolítica privilegiada. Pero también arrastra inercias burocráticas, desigualdades profundas, dependencia tecnológica y una tendencia peligrosa a reaccionar cuando ya es demasiado tarde. La historia, que rara vez perdona los errores, enseña que quienes no anticipan los cambios terminan adaptándose a ellos bajo presión, y casi siempre en condiciones desfavorables.

México e Iberoamérica enfrentan una elección clara: limitarse a ser consumidores pasivos de tecnologías diseñadas, reguladas y controladas por otros, o construir capacidades propias desde una visión estratégica compartida. La primera opción es más sencilla. La segunda, más compleja. Pero solo una de ellas abre la puerta a una soberanía real, a una seguridad auténtica y a un futuro con posibilidades.

Referencias

- Banco Mundial. (2021). World development report 2021: Data for better lives. Banco Mundial.
- Buzan, B., Waeber, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.
- Castells, M. (2009). Comunicación y poder. Alianza Editorial.
- Comisión Económica para América Latina y el Caribe [CEPAL]. (2022). Perspectivas económicas de América Latina 2022: Hacia una transición verde y digital. CEPAL-OCDE. <https://doi.org/10.1787/3c816b1f-es>

- Foro Económico Mundial [FEM]. (2023). The global risks report 2023 (18.a ed.). World Economic Forum.
- Gobierno de México. (2020). Programa para la seguridad nacional 2020-2024. Secretaría de Seguridad y Protección Ciudadana.
- Instituto Español de Estudios Estratégicos [IEEE]. (2020). Inteligencia artificial: Tecnología, aplicaciones y consecuencias para la defensa y seguridad. Ministerio de Defensa de España.
- Kaldor, M. (2012). New and old wars: Organized violence in a global era (3.a ed.). Stanford University Press.
- Ministerio de Defensa de España. (2021). Estrategia de seguridad nacional 2021. Gobierno de España.
- Naciones Unidas. (2021). Hoja de ruta para la cooperación digital: Recomendaciones del Panel de Alto Nivel del Secretario General sobre la Cooperación Digital. Naciones Unidas.
- Nye, J. S. (2011). The future of power. PublicAffairs.
- Organización del Tratado del Atlántico Norte [OTAN]. (2022). NATO 2022 strategic concept. NATO. <https://www.nato.int/strategic-concept/>
- Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2019). Artificial intelligence in society. OCDE Publishing. <https://doi.org/10.1787/eed-fee77-en>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2021). Recommendation on the ethics of artificial intelligence. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- RAND Corporation. (2020). Implications of artificial intelligence for nuclear deterrence stability. RAND Corporation.
- Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.
- Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.
- Schwab, K. (2016). La cuarta revolución industrial. Debate.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
- Stockholm International Peace Research Institute [SIPRI]. (2023). SIPRI yearbook 2023: Armaments, disarmament and international security. Stockholm International Peace Research Institute.



CAPÍTULO NOVENO

MÉXICO, COLEGIO DE DEFENSA NACIONAL (CODENAL)

Escenarios futuros de las operaciones militares en Iberoamérica

Edgar Ortiz Arellano

Resumen: Las tecnologías avanzadas en el futuro tendrán un papel decisivo en la forma, diseño y realización de las operaciones militares, en el marco de un contexto marcado por la incertidumbre y la constante aparición de innovaciones que generan ventajas o asimetrías en las capacidades de las Fuerzas Armadas, de ahí que el objetivo de este trabajo fue el de construir escenarios al 2040 de las operaciones de las Fuerzas Armadas de la región iberoamericana a partir de la identificación de factores claves. El procedimiento prospectivo arrojó cuatro escenarios, de los cuales dos relativamente favorables en cuanto a las capacidades estratégicas y las transformaciones que las tecnologías provocan en las operaciones militares. Además, se realizaron dos escenarios disruptivos a partir de la ubicación de señales débiles y antagonismos proyectados al futuro. Entre las recomendaciones resalta que Iberoamérica debe comenzar a reducir las asimetrías económicas y militares con el fin de que los cambios acelerados en la tecnología no le mermen sus capacidades defensivas y de seguridad.

Palabras clave: Capacidades estratégicas, escenarios, futuros posibles, guerra, tecnología.

Acerca del autor: Edgar Ortiz Arellano es doctor en gestión estratégica y políticas del desarrollo, actualmente se desempeña como docente-investigador en el Colegio de Defensa Nacional (México). Es miembro del comité asesor del Seminario Universitario de Estudios sobre Democracia, Defensa, Dimensiones de la Seguridad e Inteligencia de la Universidad Nacional Autónoma de México y miembro de la Red Iberoamericana de Prospectiva.

Introducción

El futuro de la humanidad se determina en el presente a partir de las capacidades que se logren desarrollar en el ámbito de las tecnologías avanzadas y su aplicación en aquellos sectores estratégicos que son los que determinan el éxito o fracaso de una sociedad. La defensa de los Estados-Nación ante amenazas externas e internas no está exenta de los impactos que la revolución tecnológica trae consigo. Ahora las Fuerzas Armadas requieren de sofisticación en su entrenamiento, equipamiento y formas innovadoras para realizar sus operaciones de forma exitosa, debido a que el mundo se ha convertido de manera acelerada en un espacio complejo y competitivo, así que las respuestas y previsiones con respecto al mañana se deben construir, reconstruir y reinventar constantemente.

La tecnología en la actualidad, en las sociedades postindustriales, no solo determina ciertos procesos productivos, reorganiza y estructura las relaciones sociales, las formas y métodos de organización económica (Marcuse, 2019), tal como en la toma de decisiones de índole estratégica para el Estado. Ante las condiciones de incertidumbre y de constantes cambios, imprevistos en las relaciones y equilibrios de poder, es necesario repensar las estrategias y líneas de acción de cara a diferentes escenarios que, en los próximos quince años, podrían sucederse para Iberoamérica. Las previsiones sobre el mañana no son predicciones ni hechos con plena certeza de su ocurrencia, pero sí son indicativos de cómo evolucionarían ciertos factores que son portadores de futuros y que tendrán un rol preponderante en una temporalidad en el futuro. Es un hecho que la tecnología tiene impacto en el campo de poder militar, pero los derroteros que asuma pueden ser inciertos en buena medida por circunstancias ajenas a la propia tecnología y a la dinámica de las Fuerzas Armadas.

Ante la necesidad de proyectar el futuro como instrumento estratégico del Estado, el presente ensayo tiene como objetivo construir escenarios al 2040 de las operaciones de las Fuerzas Armadas de la región iberoamericana a partir de la identificación de factores claves que influyen en el objeto de estudio. Para lograr la meta de este trabajo, se realizó una primera fase de contexto, otra visualización estratégica y una tercera con la creación de escenarios (Gándara, 2024), y se presentan recomendaciones y conclusiones, con énfasis en la necesidad de la región de incorporar de forma inmediata dos puntos: 1) tecnología de punta como apoyo para la toma de decisiones, y 2) un sistema de desarrollo e innovación permanente en las estructuras militares para evitar asimetrías significativas con otras regiones.

Contexto actual

Nicolas Taleb (2007), a principios de la década pasada, propuso la categoría de análisis de “cisne negro”, que es un acontecimiento impredecible, poco probable de ocurrencia, pero con gran impacto, con la característica de una vez que sucedido el evento, se generan narrativas explicativas de él, que hacen parecer que pudo preverse, pero la realidad es que su característica es que no lo es. En este sentido, la tecnología, debido a la velocidad con la que se aplica en las diferentes esferas de la vida y las posibles ventajas que puede generar en el diseño y realización de operaciones militares, acentúa la generación de cisnes y de los ambientes perfilados como volátiles [volatile], inciertos [uncertain], complejos [complex] y ambiguos [ambiguous] (VUCA). La tecnología aporta en la actualidad un mundo más conectado, pleno de datos e información, mejoras en diferentes industrias, en la exploración y apropiación del espacio exterior, en adelantos médicos y, obviamente en mejoras en el armamento militar, que se vuelve más letal y preciso.

Esta condición VUCA modifica las formas de hacer la guerra y la acelerada irrupción de la tecnología, obliga a que la organización de las operaciones militares considere estos dos componentes en el arte y diseño operacional, el arte entendido como el “proceso creativo que tiene por objeto visualizar la mejor manera de emplear capacidades militares conjuntas y combinadas, en el nivel operacional de la guerra, y el empleo eficaz de fuerzas militares para lograr

objetivos operacionales y estratégicos, por medio del diseño y conducción de la campaña,” (Keny, *et al.*, 2017: p. 23).

El proceso creativo de los comandantes y jefes estará reforzado por el uso de tecnologías analíticas y la toma de decisiones será más acelerada, además de que se apoyará de simuladores y otros instrumentos. Por otra parte, al diseño operacional se le puede definir como “la aplicación de pensamiento crítico y creativo –en el nivel operacional– para conocer, visualizar y describir problemas complejos y gestar aproximaciones para su solución” (Keny, *et al.*, 2017: p. 24). Nuevos dominios y condiciones más complejas enfrenta el diseño operacional; esto implica que a mayor sofisticación de los adversarios también requerirá planes y diseños elaborados bajo lógicas de precisión en los objetivos e identificación de los centros de gravedad del enemigo y propios, pero sobre todo con la consideración de los cambios, ventajas y alteraciones que un dispositivo tecnológico puede tener en los cursos de acción.

La guerra, como forma de competencia, según Lodhi, *et al.*, (2025), carece, en la actualidad, de una autoridad central que brinde protección y se rige por la anarquía del sistema internacional. En una competencia por el poder, los Estados intentan asegurar su supervivencia dentro del sistema. Para lograrlo, buscan obtener una ventaja competitiva y mayor influencia mediante la adquisición de herramientas que resultan más efectivas en relación con sus costos políticos y militares; en este sentido, la tecnología brinda esos instrumentos, tecnologías y dispositivos que ayudan a la sobrevivencia de una nación.

Las tecnologías que en este momento tienen la primacía son la biotecnología, la inteligencia artificial, semiconductores, tecnologías cuánticas y espaciales. Estados Unidos de América (EE.UU.), es el país puntero en el desarrollo de estas tecnologías, seguido de cerca de China, Europa, Japón y Corea del Sur (Harvard Kennedy School, 2025). La forma en la que se desarrolla la tecnología y la tendencia que asume “reflejan intrínsecamente las normas, las ambiciones y los conflictos sociales. Los seres humanos (ya sean inventores, inversores o responsables políticos) definen qué problemas deben abordar las tecnologías y las diseñan para ofrecer soluciones” [traducción propia] (Winkler, 2025: p. 3). Pero la tecnología en sí misma es un campo de poder que entra en el espectro de las luchas híbridas, pues un país o región que carece de ella no podrá ser competitivo en ningún aspecto, especialmente el militar. Por ejemplo, para la

libertad (relativa) de acción en el aire, el espacio y el ciberespacio, del mismo modo para la realización de operaciones conjuntas en todos los dominios, es necesario contar con un apoyo tecnológico, pero esto implica tener conciencia de que la superioridad tecnológica está limitada en el tiempo y el espacio, lo que requiere de un enfoque estratégico para seguir en la innovación y con ello generar ventaja en todos los dominios de la guerra de forma sostenida (Schweiker, 2026).

La aplicación de innovaciones en el campo militar se puede dirigir hacia cuatro áreas relevantes; la primera es la conectividad en cuanto a las formas en que los combatientes detectan y localizan a sus enemigos, junto con las comunicaciones para realizar y dirigir las operaciones. La segunda tiene que ver con la letalidad; esto implica el daño que las armas y los sistemas de armamentos pueden infligir en el campo de batalla. El tercer factor tiene que ver con el ya mencionado uso de armas autónomas con IA y su implementación también en la toma de decisiones en los niveles estratégicos, tácticos y operativos. La cuarta área es la sostenibilidad, que se refiere a las capacidades que tienen las Fuerzas Armadas para abastecer y apoyar a las tropas desplegadas en diversas operaciones (ODNI, 2021).

La tecnología se puede aplicar a cualquier nivel de la conducción de una operación militar, es decir, el estratégico, operativo, así también en el táctico y su categorización dependerá del impacto que esta tenga en la consecución de los objetivos que se pretenden obtener (Secretaría de la Defensa Nacional, 2017: pp. 3-4). Un implemento tecnológico puede ayudar a los niveles estratégicos a tomar decisiones que impacten en el largo plazo al Estado o a sus instituciones; en el plano operativo, ayuda a los mandos militares a diseñar y darle seguimiento a las acciones de las tropas y, en el nivel táctico, se pueden convertir en armas o apoyo sobre el terreno de las operaciones. Una ventaja que brinda la tecnología en el presente y en el futuro es la rapidez con la que se realiza alguna medida o se evalúa una situación en el teatro de operaciones, como por ejemplo, las condiciones climáticas, caminos e infraestructura, población, orografía e hidrología, comunicaciones, etcétera. En tiempo real in situ se recolectan datos que en segundos son analizados para determinar qué hacer mientras suceden las operaciones. Al planear la operación, se determinan las opciones de los cursos de acción que serán diseñados por simuladores de tecnología

cuántica o IA generativa y ya no por un diseñador humano (o por lo menos esa es la tendencia).

Las tecnologías aplicadas a las operaciones militares, son variables dependientes del gasto en investigación y desarrollo que cada país realice con respecto a su Producto Interno Bruto (PIB), así como del stock de capital de tecnologías de la información y la comunicación (TIC). Con respecto al gasto en investigación y desarrollo, el Banco Mundial (2026) informa que América del Norte (en particular los Estados Unidos de América) es la región que más invierte, con un porcentaje de 3.3. Con relación al PIB, seguido de Asia Oriental y Pacífico con 2.77 por ciento de gasto, seguida de la Unión Europea con un 2.26 de gasto promedio; América Latina alcanza un 0.7 por ciento, cifra que está por debajo de la media mundial que es de 2.59. Asia Meridional y el África al sur del Sahara presentan niveles del 0.63 y 0.44 por ciento respectivamente (véase figura 1).

Es importante considerar una tercera variable: el gasto militar. Según el Defence Technology Sector Report del Clairfield International GmbH., (2025), los países con mayor gasto son los 1) EE.UU.; 2) China; 3) Rusia; 4) Alemania; 5) India; y 6) Reino Unido. Estos países tendrán el reto, además de la competencia global en la que se encuentran por la hegemonía; es el hecho de mantener el equilibrio entre su poderío militar y las capacidades económicas, con el fin de no caer en su proceso de decadencia acelerada.

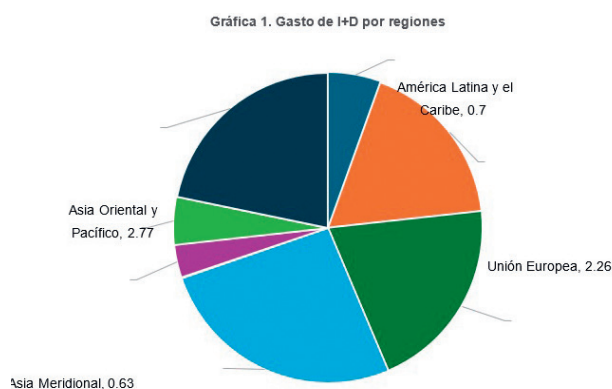


Figura 1. Fuente: Banco Mundial (2026). Elaboración propia.

En el caso de Iberoamérica está el dilema de gastar en asuntos militares o invertir los recursos en desarrollo; sin embargo, como criterio de decisión, es que existen una serie de amenazas emergentes como lo es el crimen organizado transnacional que utiliza tecnología como la IA, drones, minas, sistemas de comunicación y de video vigilancia avanzada, entre otros dispositivos para su actividad criminal. El no invertir en las Fuerzas Armadas de la región podría colocar en desventaja al Estado frente a diversos agentes hostiles y podría ser un espacio atractivo para diversas amenazas como lo son los grupos terroristas o de extremismo ideológico, que, al observar la debilidad de las fuerzas de la seguridad y defensa, se asientan en ella y la convierten en su centro de acción delictiva.

La guerra es una realidad más que vigente y, paradójicamente, en un mundo interdependiente en lo comercial y financiero, el ideal de paz global se observa más complicado. El realismo político se materializa en conflictos convencionales, amenazas híbridas (entendidas como la combinación de recursos económicos, políticos, tecnológicos, diplomáticos y de comunicación, así como militares con fines hostiles sobre otros Estados), guerra irregular y, por supuesto, ciberataques instalaciones críticas físicas y virtuales, entre otras formas de conflicto entre Estados y agentes no estatales. Esta situación obligará a cambiar el sistema de educación militar hacia el fortalecimiento de las habilidades del pensamiento, como lo son el pensamiento crítico, la abstracción y la problematización, pero también hacia el uso y manejo de herramientas tecnológicas que hagan más eficientes las operaciones y se logre, con los recursos que se cuentan, alcanzar el estado final deseado planteado para cada misión.

La sociedad global ha entrado a las guerras de sexta generación, donde la lucha será multidimensional, con grandes cantidades de datos por procesar para conocer a detalle las especificidades de los enemigos o de los objetivos que se pretenden atacar. Este tipo de conflicto está estrechamente ligado a la guerra de información, psicológica y las de tipo irregular. Sus armas se lanzan desde plataformas terrestres, marítimas, aéreas y espaciales (Jijan & Fadel, 2025). Esta forma de acción bélica pretende operar la gestión de la información para provocar conflictos económicos; sus estrategias operan a larga distancia.

Con el uso de la tecnología se podrán implementar métodos de ataques electrónicos los cuales buscan penetrar sistemas informáticos, redes, sistemas de comunicación, y extraer, destruir o inhabilitar información. Esto se logra mediante el uso de diversos medios, como virus, malware o ataques maliciosos. También influirán los métodos de dispersión de información falsa, por ejemplo, a través de las redes sociales con el fin de bajar la moral, inhabilitar el liderazgo de los decisores político-estratégicos o simplemente generar caos (Jijan & Fadel, 2025).

Es de especial atención el creciente uso de la IA en las operaciones militares, debido a que con ella se podrán realizar operaciones de manera simultánea en los diferentes dominios, pero, por otra parte, también las Fuerzas Armadas deberán considerar las operaciones cibernéticas que pueden tener capacidad para interrumpir las cadenas de suministros y la logística militar. La desinformación masiva provocada por las campañas que pretenden influir en la opinión pública y en la moral de las tropas (Scott, 2026). También se podrían entorpecer las operaciones de inteligencia y de contrainteligencia, así como atacar los sistemas financieros y de servicios básicos a la población con el fin de generar inestabilidad social que entorpecería las capacidades de gobernabilidad. Se prevé que el mercado mundial de IA en el ámbito militar alcance los 35,200 millones de dólares en 2031 y en los ámbitos que principalmente se destinan recursos son: 1) procesamiento de información con un 46.1 por ciento; sistemas aéreos no tripulados 19 por ciento; ciberseguridad 16.2 por ciento; otros 11 por ciento; logística 7.3 por ciento (Sandal, 2025).

La IA en poco tiempo se instalará en casi todos los aspectos militares y las operaciones que realicen las Fuerzas Armadas de Iberoamérica no serán la excepción, en buena parte, porque se convierte en una oportunidad para disminuir las asimetrías que en el campo de poder militar presenta la región con respecto a las potencias en ese rubro como lo son EE.UU., Rusia y China, y a otras regiones, como la Unión Europea y Asia- Pacífico. Habid, *et al.* (2026) señalan que:

Los avances en aprendizaje automático, visión artificial, análisis de macrodatos y sistemas automatizados de apoyo a la toma de decisiones han trascendido el uso civil y se han integrado en las funciones básicas de las Fuerzas Armadas,

lo que ha transformado la preparación, la conducción y el control de la guerra [traducción propia] (p. 58).

El espectro de acción de la tecnología no se reserva sólo a IA y a sus muchas aplicaciones, los avances técnicos para uso militar, según Wallner (2026), se decantan en diez temas prioritarios: 1) integración de la IA; 2) ciberseguridad y guerra cibernética; 3) eficiencia energética y sostenibilidad; 4) sistemas de armas autónomos; 5) tecnologías inmersivas; 6) internet de las cosas militares; 7) conectividad 5G; 8) guerra electrónica; 9) biotecnología y 10) mejora humana. Como se puede observar, algunos de los temas son apoyo logístico, otras tantas mejoras en la capacidad letal del armamento y en el desempeño de las tropas con la meta de ser eficientes en su actuar y en sus capacidades humanas.

Un tema en el que Iberoamérica debe considerar su pronta inclusión, es el del espacio ultraterreno como un dominio de acción militar; si bien la región tiene presencia con satélites de uso civil, en los próximos años, la infraestructura militar se expandirá con el fin de apoyar las operaciones militares. Armas láser (Zhang et al 2023), cinéticas (Li, et al., 2026), tectónicas (Bychkov, 2023), de plasma (Eslami 2026), meteorológicas (Terebiński, 2024), antisatelitales, sistemas antimisiles, sistemas de detección de enemigos, entre otras tecnologías (Opran, 2020), serán en el futuro próximo una realidad operativa e instaladas en el espacio, las cuales brindarán una ventaja sin precedentes a los países que los utilicen. Para las nuevas tecnologías en el ámbito militar, no hay frontera que no pueda sobrepasar ni ámbito material, virtual e inmaterial que no se convierta en un potencial campo de batalla. En esta lógica, la conquista del espacio y de la órbita terrestre es importante y estratégica para lanzar operaciones a gran distancia y con precisión, sobre objetivos que, simplemente en una posición terrestre, serían inalcanzables.

Visualización estratégica

Para determinar los escenarios que pueden asumir las operaciones militares en Iberoamérica, como resultado de la irrupción acelerada de nuevas y avanzadas tecnologías, es necesario determinar, a partir del contexto planteado, las tendencias, las señales débiles y las variables estratégicas.

En primer lugar, las tendencias globales que se pueden ubicar son cinco: 1) transición hacia guerras de sexta generación; 2) integración de la IA en todos los ámbitos; 3) uso del espacio ultraterrestre para fines militares; 4) prevalencia de guerras híbridas y ciberataques; 5) desarrollo de armas autónomas. En segundo lugar, se tienen como señales débiles, entendidas estas como indicadores tempranos de cambio: 1) aparición de tecnologías militares sofisticadas (cinéticas, ambientales, de plasma, electromagnéticas); 2) sustitución del diseñador de operaciones militares por parte de la IA; 3) biotecnología para la mejora humana; 4) acceso a la tecnología militar por parte de actores no estatales. Entre las variables claves que pueden ser consideradas para el futuro están:

1. el gasto en investigación y desarrollo;
2. el gasto militar bruto;
3. la orientación de la educación militar;
4. el equilibrio entre economía y fuerza militar;
5. ventaja tecnológica sostenida.

Megatendencias	Señales débiles	Variables claves
Guerras de sexta generación	Tecnologías militares sofisticadas.	Gasto en investigación y desarrollo.
Uso intensivo de la IA en aspectos militares	Diseñador de operaciones militares con IA.	Gasto militar.
Espacio ultraterrestre para fines militares	Biotecnología para la mejora humana.	Educación militar.
Guerras híbridas y ciberataques	Tecnología militar por parte de actores no estatales.	Equilibrio entre economía y desarrollo militar.
Desarrollo de armas autónomas		Ventaja tecnológica sostenida.

Tabla 1. Factores claves para la creación de futuros de las operaciones militares en Iberoamérica. Fuente y elaboración propia.

Aunado a estos tres grupos de factores que se pudieron inferir a partir del contexto que se presenta en este documento, el World Economic Forum (WEF) considera a los siguientes nueve factores, como riesgos relevantes para los próximos diez años: 1) desinformación y noticias falsas, 2) consecuencias adversas de las tecnologías de IA, 3) inseguridad cibernética, 4) conflictos armados entre Estados, 5) concentración de recursos y tecnologías estratégicas, 6)

confrontación geoeconómica, 7) armas o peligros biológicos, químicos o nucleares, 8) consecuencias adversas de las tecnologías de vanguardia, 9) violencia intraestatal (2026: p. 14). En su conjunto, se pueden categorizar los antagonismos en cuatro ejes: 1) amenazas y riesgos tecnológicos; 2) amenazas y riesgos geopolíticos y estratégicos; 3) amenazas de armas de destrucción masiva; 4) violencia interna y social. Estos riesgos y amenazas se constituyen en antagonismos a la seguridad nacional de los Estado-Nación de Iberoamérica y su acción conjunta en un escenario al 2040 podría constituir un escenario catastrófico para el mundo y en particular para la región: estos antagonismos se usaron para la creación de los escenarios disruptivos.

Escenarios con Ejes de Schwartz

Para crear escenarios posibles, se decidió implementar la metodología de los Ejes de Schwartz, con un horizonte de tiempo a 14 años (2040), es decir, al mediano plazo. El punto central de decisión son las operaciones militares y sus cambios o afectaciones a partir de la irrupción tecnológica con énfasis en Iberoamérica. Como fuerzas motoras están las variables claves y las megatendencias que se pueden observar en la tabla 1. Los Ejes de Schwartz a partir de la construcción de un plano cartesiano en el cual se combinan el aumento o disminución de las capacidades de los factores que están en interacción (Gándara y Farías, 2024), se crean escenarios. En el eje X se colocaron las megatendencias, este bloque representa las transformaciones de la guerra. En el eje Y se colocaron las variables que representan las capacidades estratégicas que son base del poder nacional de los países.

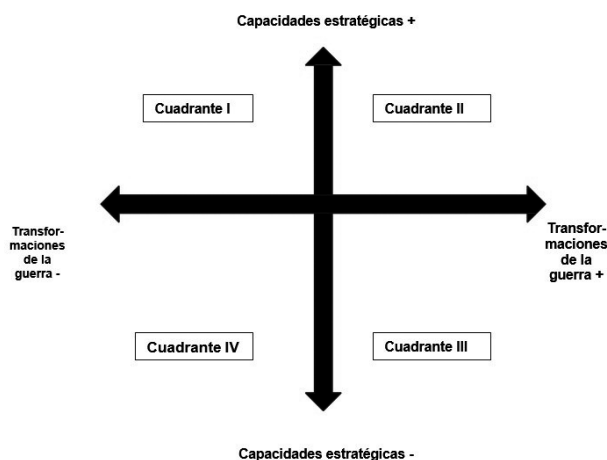


Figura 2. Fuente y elaboración propia.

En el primer escenario se combinó un aumento de las capacidades estratégicas de los Estado-Nación y una disminución de los factores que aceleran las transformaciones en los conflictos bélicos. Se le llamó a este escenario: "Fortaleza con innovación limitada".

Escenario cuadrante I. "Fortaleza con innovación limitada"

En el 2040 los países de Iberoamérica están fortalecidos en sus capacidades militares, debido a que, de forma paulatina, han logrado incrementar su gasto militar entre el dos y tres por ciento de su PIB; este crecimiento ha ido a la par de una mayor investigación y desarrollo. El sistema educativo de la región ha podido consolidarse en el marco de las nuevas tecnologías y en el entendimiento de su uso, especialmente para el diseño de las operaciones militares. Los esfuerzos en gasto y formación han producido un crecimiento sostenido suficiente para cubrir las necesidades de seguridad y defensa; sin embargo, la inclusión total de alta tecnología, avanza de manera muy lenta. Iberoamérica tiene poca participación en la apropiación del espacio ultraterreno, en la creación de armas de alta tecnología, así como en el desarrollo de armas autónomas. Las Fuerzas Armadas se preparan para realizar operaciones ante amenazas híbridas, pero la tecnología sigue incipiente. El uso masivo de la IA está en

un nivel intermedio y es implementada especialmente en el nivel político estratégico, pero no se ha incorporado plenamente en los niveles operativos y tácticos.

Las operaciones militares en la región tienen un importante nivel de sofisticación, pero son cercanas a modelos tradicionales. Existe estabilidad en la región, mas se pueden detectar vulnerabilidades, como consecuencia de adelantos tecnológicos propios o por lo menos incorporados en las estructuras organizacionales de las operaciones, las cuales ponen en riesgo al Estado frente a fenómenos o antagonismos disruptores. En general, sí hay una transformación operacional, pero de carácter limitado.

Escenario cuadrante II. “Transformación operacional plena”

Este escenario combina un alto nivel de transformaciones en todos los ámbitos de las formas que pueden asumir los conflictos bélicos y, por lo tanto, las operaciones, pero también un aumento en las capacidades estratégicas de la región:

En 2040, Iberoamérica alcanza un nivel de madurez estratégica gracias a la inversión sostenida en investigación y desarrollo de tecnología, junto con una educación militar moderna y plena en el desarrollo de innovación y capacidad creativa, lo cual ha potenciado el poder nacional de los países de la región. Las capacidades estratégicas se han fusionado y adaptado a las transformaciones que la tecnología genera en las operaciones y en las concepciones que se tienen con respecto a la seguridad y defensa. Las operaciones militares han cambiado radicalmente con respecto a sus predecesores de hace 14 años.

Las Fuerzas Armadas de la región integran sistemáticamente la IA en los niveles estratégicos, operativos y tácticos. Existen capacidades de despliegue de sistemas de armas autónomas en operaciones conjuntas y utilizan el espacio ultraterrestre como un dominio militar activo. Las guerras híbridas y los ciberrataques están considerados como antagonismos calculados y con las medidas preventivas consideradas en la doctrina militar. La ventaja tecnológica sostenida permite realizar campañas multidominio, lo cual da grandes capacidades operativas a la región.

La toma de decisiones se realiza con velocidad y la tecnología ha generado mayores capacidades disuasivas; ambas circunstancias han redefinido el equilibrio global. Iberoamérica se proyecta como un bloque capaz de competir con otras regiones y se constituye en una fuerza defensiva relevante para el hemisferio. Las amenazas de actores no estatales y de conflictos que en su momento se conocían como de sexta generación siguen vigentes y pueden vulnerar a los Estado-Nación en cualquier momento, pero existe la ventaja de que se pudo lograr la combinación de capacidades estratégicas sólidas, con el uso acertado y oportuno de la tecnología en las operaciones militares.

Escenario cuadrante III. “Modernización asimétrica”

Este escenario se caracteriza por la disminución de las capacidades estratégicas y un aumento de las transformaciones en el ámbito militar global:

En 2040, Iberoamérica se enfrenta a una serie de amenazas de tipo cibernético e híbridas que usan diversas tecnologías para minar las capacidades del Estado. La IA y las armas autónomas se han integrado a las operaciones militares, pero con muchas deficiencias y limitaciones debido a que no se cuenta con el presupuesto adecuado, lo mismo sucede con la investigación y el desarrollo que no superan el 0.07 por ciento del PIB. Aunado a que no existe un sistema educativo acorde a las aceleradas innovaciones tecnológicas, lo que ha obligado a que de forma improvisada se aprenda el uso de la poca tecnología con la que se cuenta. Existen desequilibrios entre gasto para defensa e inversión en desarrollo económico, lo que hace más frágiles a los Estado-Nación.

Las operaciones militares se ven afectadas de forma negativa, debido a que actores estatales ajenos a la región y no estatales aprovechan la tecnología para vulnerar las capacidades de las Fuerzas Armadas y con ello a la estabilidad del Estado. Existe una dependencia de la región hacia las potencias mundiales para conseguir tecnología, por lo que es difícil de operar debido a que no se cuenta con la doctrina, la infraestructura y capacidades técnicas adecuadas.

Se intenta integrarse a la modernización tecnológica, pero por las carencias estructurales, esta situación se convierte en una debilidad que termina en subordinación ante diversos actores ajenos al interés nacional de los países de

Iberoamérica. Las operaciones están desarticuladas y en muchas ocasiones son poco eficaces; además, se corre el riesgo de perder autonomía en la conducción militar.

Escenario cuadrante IV. “Inercia y rezago operacional”

El presente escenario se basa en una disminución tanto de las capacidades estratégicas como en las transformaciones en las operaciones militares como resultado de la incorporación de la tecnología en las Fuerzas Armadas de Iberoamérica:

En el 2040, la región iberoamericana atraviesa un debilitamiento estructural en relación con sus capacidades militares. El gasto militar se ha reducido de forma constante y la investigación y el desarrollo se encuentran estancados por falta de recursos que alienten la innovación y la producción de tecnología propia. Existen algunos esfuerzos aislados por generar cambios sustantivos en las capacidades militares que puedan ser aplicadas a las operaciones, pero no se vislumbra una sistematización de ventajas sostenidas en ese ámbito, esto debido a los desequilibrios que hay en otros ámbitos como el económico y social, que son prioridad para los gobiernos.

Los cambios en las operaciones militares para incorporar tecnología avanzan lentamente o se encuentran estancados. La IA no es explotada de manera intensiva y se usa ocasionalmente en el diseño operacional. Los sistemas de armas autónomas están en fase experimental (en Iberoamérica) y aquellos que son funcionales son demasiado costosos para los estándares de la región. Las amenazas híbridas y los ciberataques son gestionados por medios tradicionales y sin una infraestructura de apoyo. No hay presencia de Iberoamérica en el espacio ultraterrestre en ningún aspecto militar y se considera un actor marginal en el ámbito civil.

La región se mantiene en cuanto a sus operaciones en un nivel convencional, con limitadas capacidades, lo que genera un rezago estratégico y trae consigo que se encuentre vulnerable ante diversas potencias globales y actores no estatales. La relevancia militar de Iberoamérica es menor, dado que circunscribe a un plano reactivo frente a otros competidores y antagonismos.

Hacia escenarios disruptivos

Los escenarios anteriores muestran futuros alternativos que son posibles que ocurran a partir de las acciones que se decidan tomar en el presente. Los escenarios de los cuadrantes tres y cuatro podrían ser los tendenciales si todas las condiciones actuales siguen igual y se mantienen las inercias en relación con la inversión que se realiza en investigación y desarrollo por debajo de la media mundial. El escenario del cuadrante II, presenta una situación donde el avance tecnológico militar avanza con fuerza, pero también las capacidades para asimilarla e integrarla a las operaciones militares o, en su defecto, para tener los recursos para enfrentarla en caso de que sea usada por un agente hostil al Estado.

Para ampliar la comprensión de los futuros posibles, es necesario que se contemplen escenarios disruptivos, que están constituidos por las cuatro señales débiles y los cuatro ejes o grupos de antagonismos que ya se han indicado anteriormente. Con base en ello, se crearon dos escenarios disruptivos que se consideran como poco probables, pero en caso de realizarse serían de alto impacto para la región.

Escenario disruptivo “Salto inesperado”

Iberoamérica en 2040 experimenta un súbito despliegue de tecnologías avanzadas militares. Las armas cinéticas, meteorológicas, de plasma y electromagnéticas se incorporan en programas regionales de defensa. La inteligencia artificial sustituye a los encargados de diseñar las operaciones y acciones militares, pero bajo esquemas doctrinales que mantienen cohesión y control humano. La biotecnología es aplicada a la mejora del personal militar con respecto a su resistencia física y capacidad cognitiva. Los actores no estatales tienen acceso a la alta tecnología, aunque la región logra construir mecanismos de cooperación y disuasión inéditos, lo que provoca que se convierta en un actor inesperadamente competitivo en el sistema internacional.

Escenario disruptivo “Tecnología sin control”

En 2040, Iberoamérica enfrenta un panorama de irrupción de tecnologías militares avanzadas. Las diversas armas que alguna vez solo fueron diseños futuristas o ficción, se han convertido en una realidad y se distribuyen sin regulación alguna, lo que genera una carrera armamentista y no existe una coordinación regional. La IA sustituye a los diseñadores y conductores de las operaciones militares, pero lo hace sin marcos doctrinales, ni supervisión humana, lo que conlleva a decisiones opacas, vulnerables a manipulación de diversos intereses ajenos al Estado y distantes de criterios éticos. La biotecnología aplicada a los humanos, junto con la tecnología avanzada, creó a nivel mundial y regional ejércitos de élites frente a ejércitos convencionales. De forma simultánea, actores no estatales tienen acceso a tecnologías militares sofisticadas y las emplean en conflictos híbridos, ciberataques masivos y operaciones transnacionales que superan al Estado.

Incertidumbres

Los ejes de Schwartz propusieron cuatro escenarios que pueden ser catalogados como lineales, es decir, no hay elementos disruptivos que pudiesen cambiar su trayectoria hacia el 2040, pero la realidad empírica señala que las condiciones VUCA y la aparición de cisnes negros (Taleb, 2007) pueden hacer cambios de forma disruptiva, de ahí que se propusieran dos escenarios disruptivos, que pueden ser considerados como extremos y que en todos los análisis deben estar presentes. Aunado a los seis escenarios que ya se han planteado, se sugiere considerar tres grandes incertidumbres, entendidas como los factores externos que están fuera del alcance del decisor (Marchau, 2019): 1) La evolución de la competencia geopolítica por la hegemonía global; 2) posible empoderamiento de actores no estatales; 3) impacto de los cisnes negros sobre el sistema global.

En el primer caso, los países hegemónicos están en competencia por el control de los recursos críticos (por ejemplo, tierras raras) para el desarrollo tecnológico. (Middleton, 2026), y esta situación es un incentivo para generar dependencia tecnológica que puede afectar a Iberoamérica. Con respecto al acceso de tecnología militar por parte de agentes no gubernamentales, el interés

radica en monitorear especialmente al crimen organizado transnacional en sus diversas modalidades, al terrorismo y al extremismo ideológico. Estos grupos antisistema, en la actualidad, han mostrado capacidades para usar tecnología con fines criminales (como es el caso del empleo de drones), por lo que se deberá dar seguimiento al control de esta tecnología. El tercer aspecto son los ya mencionados cisnes negros, que pueden especialmente aparecer en el campo económico y con ello afectar el desarrollo de la región y nuevamente provocar fuertes desequilibrios. Estas tres incertidumbres deberán ser vigiladas de forma constante, junto con el grupo de antagonismos que se detectaron en esta investigación.

Recomendaciones

Con base en el escenario del cuadrante II que es considerado el más positivo, se propone una serie de recomendaciones que son de aplicación general en la región y en particular en el hemisferio occidental.

1. Gasto en investigación y desarrollo. Es necesario que la región, de forma estructural, cambie la composición presupuestal con el objeto de aumentar la proporción del PIB destinado a la investigación y desarrollo científico, especialmente hacia aplicaciones tecnológicas, con el fin de que se aproveche el talento humano y la innovación que se genere en los diversos países iberoamericanos.
2. Gasto militar. Es indispensable que, de forma escalonada el gasto militar crezca hasta alcanzar la proporción del dos por ciento del PIB como mínimo, con el fin de contar con tecnología y equipamiento que apoye las operaciones militares de las Fuerzas Armadas de la región y mantener un crecimiento sostenido en poderío militar.
3. Sistema educativo militar. Se debe modernizar el sistema educativo militar de la región para preparar a las Fuerzas Armadas en un entorno tecnológico complejo, lo que implica una formación en el uso de las tecnologías avanzadas, tanto civiles como militares, y sus aplicaciones en las operaciones. También la doctrina militar se deberá adaptar a los escenarios de amenazas híbridas, ciberataques y ciberguerra, bajo la consigna

del constante surgimiento de nuevos antagonismos (especialmente de actores no estatales), así como de nuevas armas con alta letalidad.

4. Innovación sostenida. Para que la región pueda cambiar los equilibrios de poder global a su favor, debe mantener procesos de innovación sostenida con el fin de estar a la vanguardia tecnológica y convertirse en un centro de desarrollo, inversión y creación de innovaciones científicas.
5. Nuevos dominios. Iberoamérica debe considerar el conocimiento, adaptación e incursión en nuevos dominios, como lo son el ciberespacio y el espacio ultraterreno. Las próximas guerras y amenazas del futuro se desarrollarán en esos dominios y es importante que sean incluidos en los diseños de las operaciones militares y en la planeación de la seguridad nacional y defensa exterior de los Estado-Nación de la región.

Conclusiones

Los escenarios con horizonte al 2040, de las operaciones militares de los países de Iberoamérica, se caracterizan por tener múltiples rutas a partir de la forma en que las tendencias dominantes predominan a partir de su interacción. En esta lógica, los Ejes de Schwartz arrojaron cuatro escenarios, los primeros marcados por un aumento de las capacidades estratégicas de las Fuerzas Armadas de la región; eso implica procesos educativos, investigación y desarrollo sostenido, recursos materiales suficientes para la constante adaptación a los cambios provocados por la tecnología. El escenario del cuadrante dos podría significar el mejor posible, debido a que, por una parte, se cuentan con capacidades institucionalizadas de formación, adaptabilidad y recursos suficientes; también se ha logrado obtener las habilidades necesarias para asegurar una innovación sostenida y una inclusión adecuada de la tecnología en todos los aspectos de las operaciones militares.

Se desarrollaron dos escenarios que no son tan favorables para la región, pues en ambos casos las Fuerzas Armadas se encuentran en desventaja, producto de las inercias que las debilitan y que se pueden apreciar en el presente, como lo son bajo presupuesto, la falta de innovación, dependencia tecnológica, visión convencional de la guerra. En estos escenarios, la tecnología puede abrumar y convertirse en un adversario para las Fuerzas Armadas,

tanto por su incomprensión de cómo usarla o simplemente por no poseerla. En ese sentido, es necesario tomar medidas inmediatas ante esos futuros alternativos. También se efectuaron dos escenarios disruptivos, poco probables de ocurrencia, pero que de realizarse provocarían grandes afectaciones en las operaciones militares. Uno, con un perfil positivo que implica que Iberoamérica es un polo de la tecnología militar y un eje de poder global, y otro donde la tecnología suplanta al decisor y al diseñador de las operaciones militares, sin ninguna restricción, además de tener una profunda dependencia de agentes externos a la región, y con antagonismos no estatales en posesión de armas y equipo sofisticado.

Las operaciones militares realizadas por los países iberoamericanos, tienen retos relevantes para que en el futuro estén en condiciones de enfrentar esta hipertecnificación de la vida humana y de las formas en la que pueden ser vulnerados sus países. Se deberán concentrar los esfuerzos en la reducción de las asimetrías tecnológicas y operativas con respecto a otras regiones. Esto implica, un esfuerzo para aumentar el gasto militar y de investigación científica, además de adecuar el sistema educativo militar hacia el uso intensivo de todo tipo de tecnologías en un contexto de multidominios que se expanden de forma impredecible, bajo la lógica de que surgirán nuevos antagonismos cada vez más peligrosos, pero también formas más creativas para enfrentarlos.

Referencias

- Banco Mundial. (2026). *Gasto en investigación y desarrollo (% del PIB)*. Banco Mundial. <https://datos.bancomundial.org/indicador/GB.XPD.RSDV.GD.ZS>
- Bychkov, S. (2023) Tectonic weapons of mass destruction, myth or reality? *SSRN*, pp. 1-5. <http://dx.doi.org/10.2139/ssrn.4366387>
- Eslami, M. (2026). Plasma weapons and deterrence in the age of emerging military technologies. *Bulletin of the Atomic Scientists*, 82 (2), pp. 109-118. <https://doi.org/10.1080/00963402.2026.2628508>
- Gándara, G. y Farías, J. (2024). Diseño de escenarios posibles mediante el método de ejes de Schwartz, en Gándara, G. (Coord.). *Métodos Prospectivos 2. Para la exploración de futuros en empresas, ONG, gobiernos y la agenda global*. Penguin Random House, pp. 337-368.

- Habib, M., Amin, A., & Khan, A. (2026). Artificial intelligence and sixth generation warfare: legal, political, and strategic implications for global power dynamics. *Research Journal for Social Affairs*, 4(1), pp. 57-68. <https://doi.org/10.71317/RJSA.004.01.0670>
- Harvard Kennedy School. (2025). *Critical and Emerging Technologies Index*. Belfer Center. https://www.belfercenter.org/sites/default/files/2025-06/Belfer_CET_2.4.pdf
- Jijan, I. & Fadel, S. (2025). Developments in sixth generation warfare methods. *Journal of Asian Multicultural Research for Social Sciences Study*, 6 (2), pp. 20-28. <https://doi.org/10.47616/jamrsss.v6i2.604>
- Kenny, A. Locatelli, O., Zarza, L. (2017). Arte y diseño operacional. Una forma de pensar *operaciones militares*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.
- Li, Y., Gu, T. & Wan, Q. An improved black-winged kite algorithm for solving non-lethal kinetic strike parameters for moving targets. *Sci Rep* 16 (6257). <https://doi.org/10.1038/s41598-026-36642-8>
- Lodhi, A., Shahzad, S., y Noori, M. (2025). 6th generation warfare and the future of global conflict: analyzing hybrid tactics, ai, and information dominance in modern geopolitics. *Research Consortium Archive*, 4 (1), pp. 42-61. <https://doi.org/10.0000/>
- Marchau, V., Walker, W., Bloemen, P., y Popper, S. (2019). *Decision making under Deep uncertainty: from theory to practice*. Springer.
- Marcuse, H. (2019). *Tecnología, guerra, fascismo*. Ediciones Godot.
- Middleton, A. (2026). Geopolitics of rare earth elements (REE) in the Arctic: Study of evolving strategic, scholar, and media discourse. *Polar Record*, 62 (e3). doi:10.1017/S0032247425100193
- ODNI. (2021). *The future of the battlefield*. Office of the Director of National Intelligence. <https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield>
- Opran, M. (2020). War in space. *Space Infrastructures: From Risk to Resilience Governance*. <https://doi.org/10.3233/NICSP200015>
- Pleasants, S. (2026). The AI battlespace: artificial intelligence, civil stability, and the weaponization of trust. *Small JournalWars*. <https://smallwarsjournal.com/2026/05/04/the-ai-battlespace-artificial-intelligence-civil-stability-and-the-weaponization-of-trust/>

- Sandal, G. (Ed.) (2025). *The future of defence and security*. Futures Platform Publications. https://static1.squarespace.com/static/6192b02960e94236fc22acce/t/682dcb41f72b_bbd3824f0ec64/1747831651768/The+Future+of+Defence+and+Security.pdf
- Schweiker, K. (2026). *The new frontline: technology is a modern warfighting domain*. Center for Strategic & International Studies. <https://www.csis.org/analysis/new-frontline-technology-modern-warfighting-domain>
- Secretaría de la Defensa Nacional. (2017). *Manual de Planeamiento Operacional Conjunto de las Fuerzas Armadas*. Secretaría de la Defensa Nacional.
- Taleb, N. (2007). *El cisne negro: El impacto de lo altamente improbable*. Booket Paidós.
- Terebiński, B. (2024). Climate weapons – a new weapon of mass destruction? *SJ-MULF*, 213(3), pp. 43-60. <https://doi.org/10.5604/01.3001.0054.7573>
- Wallner, S. (2026). Top 10 military technology trends in 2026: AI, autonomous weapons & cybersecurity. *StartUs Insights*. https://www.startus-insights.com/innovators-guide/military-technology-trends/?utm_source=copilot.com
- WEF. (2026). *Global risks report 2026*. World Economic Forum. <https://www.weforum.org/publications/global-risks-report-2026/>
- Winkler, S. (2025). New and old Cold Wars: The tech war and the role of technology in great power politics. *Global Studies Quarterly*, (5), pp. 1-13. <https://doi.org/10.1093/isagsq/ksaf038>
- Zhang, H. Zeng, Y., and Sun S. (2023). From the development of shipborne laser weapon of U.S. navy to analyze the military requirements and countermeasures of navy. *Journal of Physics: Conference Series*, 2478, 1-10. <https://iopscience.iop.org/article/10.1088/1742-6596/2478/8/082008/pdf>



CAPÍTULO DÉCIMO

PARAGUAY. INSTITUTO DE ALTOS ESTUDIOS ESTRATÉGICOS (IAEE)

La influencia de las nuevas tecnologías en los escenarios de operaciones futuros

Edwin Ramon Martínez González

Pedro Antonio Arguello Benitez

Héctor Antonio Aguirre

Carlos Alberto Martínez Galeano

Ruth Margarita Vallejos Espínola

Resumen: Este artículo que lleva como título “La influencia de las nuevas tecnologías en los escenarios de operaciones futuros” que toma como escenario al Estado paraguayo, nos enseña que hoy, los conflictos humanos dejaron de limitarse a campos de batalla tradicionales para mudarse a un escenario invisible pero dinámico. La ventaja ya no se mide solo en armas o control territorial; se juega en la sincronización del espacio físico con el ciberespacio y, sobre todo, con nuestra propia mente. Aunque herramientas como la inteligencia artificial aceleran decisiones, la excesiva dependencia digital nos vuelve vulnerables. Nuestros servicios básicos y datos están expuestos a ciberataques constantes. Además, el uso de las redes sociales e imágenes falsas facilita una guerra silenciosa manipulando nuestras ideas y emociones para dividir a la sociedad sin disparar un solo cartucho. En este mundo hiperconectado, protegernos es un desafío de todos. El verdadero poder de un país ya no reside en sus tanques, sino en su capacidad de cuidar y potenciar el talento de su gente.

Palabras clave: Ciberespacio, Guerra silenciosa, Inteligencia artificial, Vulnerabilidad digital, Talento humano.

Acerca de los autores: Gral. Div. Aer. Edwin Ramón Martínez González, licenciado en ciencias militares, contador público, posgrado en didáctica universitaria, diplomado en contratos y adquisiciones públicas, especialización en organización, sistemas y métodos, especialización en inteligencia estratégica, especialización en historia nacional, maestría en operaciones militares, maestría en ciencias militares, maestría en organización, sistemas y métodos, maestría en administración pública, maestría en planificación y conducción estratégica nacional, maestría en administración y dirección de empresas, doctor en desarrollo y defensa nacional, doctor en defensa, desarrollo y seguridad estratégica nacional.

Cnel. (R) Dr. Pedro Antonio Arguello Benitez, licenciado en ciencias militares, licenciado en gestión de recursos humanos, posgrado en didáctica universitaria, maestría en operaciones militares, maestría en ciencias militares, maestría en planificación y conducción estratégica nacional, doctor en defensa, desarrollo y seguridad estratégica nacional.

Mg. Héctor Antonio Aguirre, Magister en Planificación y Conducción Estratégica Nacional, Lic. en Análisis de Sistemas, especializado en Ciberseguridad y Ciberdefensa, Certified Security Analyst, Ethical Hacking, Computer Hacking Forensic Investigator y tecnologías emergentes aplicadas a la Defensa. Es Fundador y CEO del CSIRT Privado LNXnetwork S.R.L., Profesor en Ciberseguridad y Ciberdefensa – IAEE, Instructor certificado de EC-Council CEH, CHFI, ECSA, CCISO entre otras.

Mg. Carlos Alberto Martínez Galeano, Magister en Ciencias de la Educación, Analista de Sistemas, Administrador de Empresas, Especialista en Auditoría Informática, Especialista en Ciberseguridad y Ciberdefensa Estratégica IAEE, Docente y Tutor IAEE, Diplomado en Inteligencia y Contrainteligencia, Diplomado en Ciberdefensa, Hacking Ético e Ingeniería Social, Consultor Privado, Especialista en Metodología de la Investigación Científica y Tutoría de Tesis.

Mg. Ruth Margarita Vallejos Espínola., Magister por el Programa de Maestría en Planificación y Conducción Estratégica Nacional (PMPCEN) del Instituto de Altos Estudios Estratégicos (IAEE), Licenciada en Administración por la Universidad Nacional de Asunción, Actualmente se desempeña como Docente Investigadora de la FCE-UNA y docente auxiliar de la carrera de Administración de la FCE-UNA.

Introducción

Las nuevas tecnologías están cambiando por completo la forma en que entendemos la seguridad en todo el mundo, y Paraguay no se queda atrás. Hoy en día, los conflictos ya no se limitan a las fronteras de aire, tierra y agua que conocemos; ahora se juegan en una frontera invisible pero muy real: el mundo digital.

Para nuestro país, este cambio de reglas significa que el ciberespacio se convirtió en el nuevo escenario donde nos toca defendernos.

Ya estamos viendo que, a nivel global, los primeros blancos de los ataques modernos no son los cuarteles, sino la infraestructura del día a día: las redes de electricidad, los bancos y los sistemas del Gobierno. Sabiendo que el riesgo es real, el Ministerio de Defensa puso en marcha la Política de Ciberdefensa Militar (2025-2030) a través de la DIGETIC, buscando blindar nuestros datos y reaccionar rápido ante cualquier amenaza en la red, pero la tecnología también se siente en el terreno. Cuidar fronteras tan enormes y complejas como el Chaco o la Triple Frontera siempre fue un desafío gigante, y hoy los drones y la vigilancia automática están cambiando la forma de patrullar.

Nuestro principal frente de batalla actual no es una guerra tradicional, sino el combate al crimen organizado, el narcotráfico y el tráfico de armas. Las bandas criminales ya usan tecnología avanzada y drones para el contrabando, lo que obliga a nuestras fuerzas de seguridad a modernizarse para no quedar en desventaja.

Para no quedarnos atrás, Paraguay empezó a actualizar sus estrategias aliándose con expertos internacionales. Gracias a acuerdos con el Comando Sur de los Estados Unidos y la Guardia Nacional de Massachusetts, los militares paraguayos se están capacitando en temas complejos como combatir el secuestro de datos (ransomware), analizar información e inteligencia táctica.

Un ejemplo claro de esto es el nuevo puente de la Ruta Bioceánica, donde se están usando sensores inteligentes para vigilar un corredor clave para nuestra economía.

Al final del día, toda esta tecnología no sirve de nada sin el talento de nuestra gente. Iniciativas como la Especialización en Ciberseguridad y Ciberdefensa

Estratégica, un programa clave del Instituto de Altos Estudios Estratégicos (IAEE), nos hacen ver que la defensa del Paraguay del mañana ya no puede ser solo la convencional. Hoy, más que nunca, necesitamos profesionales capacitados que se animen a romper las barreras de lo analógico y se metan de lleno en el mundo de la seguridad digital.

Evolución de la tecnología en los conflictos modernos

La historia de la guerra es la historia de la innovación tecnológica aplicada a la coerción, donde el éxito militar ha migrado del dominio puramente físico hacia la superioridad informacional. Durante el siglo XX, la industrialización y el poder nuclear convirtieron a la tecnología en un componente estratégico nacional. En el siglo XXI, la convergencia de la inteligencia artificial, el Big Data y la robótica ha desplazado el centro de gravedad de los conflictos hacia el ciberespacio, el espectro electromagnético y el ámbito cognitivo. Actualmente, los sistemas autónomos y la IA aceleran la toma de decisiones y reducen los riesgos humanos, configurando un paradigma multidominio altamente dinámico. Asimismo, la interdependencia digital de las infraestructuras críticas ha convertido a la ciberdefensa en un pilar de la seguridad nacional ante amenazas híbridas, mientras que la guerra cognitiva utiliza la desinformación para manipular percepciones públicas. En este escenario, la ventaja competitiva de los Estados ya no reside en poseer plataformas militares tradicionales, sino en su capacidad institucional para integrar de forma ágil la innovación, los datos y el talento humano para preservar su soberanía.

Del campo físico al entorno multidominio

El campo de batalla tradicional ha evolucionado hacia un entorno operacional multidominio caracterizado por la convergencia simultánea de capacidades físicas, digitales, espaciales y cognitivas. Esta transformación responde a la acelerada incorporación de tecnologías emergentes que han ampliado el alcance de las operaciones militares más allá de los espacios geográficos convencionales, integrando nuevas dimensiones donde la información, la conectividad y la velocidad de decisión adquieren un valor estratégico determinante.

En los conflictos contemporáneos, la superioridad militar ya no depende exclusivamente del control territorial o de la capacidad de fuego tradicional, sino de la habilidad para sincronizar efectos en múltiples dominios de manera coordinada y simultánea. Bajo esta lógica, el concepto de operaciones multidominio busca integrar sensores, sistemas de inteligencia, plataformas de ataque, capacidades cibernéticas y sistemas espaciales en arquitecturas interoperables capaces de actuar en tiempo real. La doctrina estratégica moderna sostiene que esta integración permite desarticular los sistemas de mando y control adversarios, degradar su conciencia situacional y acelerar el ciclo de decisión propio, generando ventajas operacionales decisivas (Scharre, 2018; NATO, 2021).

La expansión hacia el dominio espacial constituye uno de los cambios más significativos en la arquitectura estratégica contemporánea. Los satélites de comunicaciones, posicionamiento global, vigilancia y reconocimiento se han convertido en componentes críticos para la conducción de operaciones militares modernas. Sistemas GPS, imágenes satelitales, enlaces de datos y plataformas de observación espacial permiten coordinar fuerzas distribuidas, ejecutar ataques de precisión y mantener superioridad informacional sobre amplias áreas geográficas. Sin embargo, esta creciente dependencia del espacio también genera nuevas vulnerabilidades, ya que la interrupción o degradación de activos espaciales puede afectar severamente las capacidades militares y civiles de un Estado.

Paralelamente, el ciberespacio emerge como un dominio operacional central en los conflictos del siglo XXI. Las redes de información, infraestructuras digitales y sistemas interconectados representan tanto herramientas estratégicas como objetivos críticos de ataque. Las operaciones cibernéticas permiten ejecutar acciones ofensivas y defensivas con elevados niveles de anonimato, velocidad y alcance global, afectando infraestructuras críticas, sistemas financieros, telecomunicaciones, redes energéticas y capacidades militares sin necesidad de desplegar fuerzas físicas convencionales. En consecuencia, los ciberataques se consolidan como instrumentos de presión política, coerción estratégica y guerra híbrida capaces de alterar la estabilidad nacional e internacional.

La integración entre el dominio físico y el ciberespacio ha dado origen a nuevas formas de conflicto donde los ataques digitales complementan operaciones militares tradicionales. Un adversario puede degradar sistemas de defensa aérea mediante intrusiones cibernéticas, afectar comunicaciones tácticas o manipular sistemas logísticos antes de una operación cinética convencional.

Esta convergencia incrementa la complejidad operacional y exige desarrollar estructuras de defensa resilientes, interoperables y adaptativas frente a amenazas multidimensionales.

De manera complementaria, el dominio cognitivo adquiere una importancia creciente debido al rol central que ocupa la información en sociedades hiperconectadas. Este dominio comprende el espacio donde se forman percepciones, opiniones, creencias y procesos de toma de decisiones individuales y colectivas. En el entorno digital contemporáneo, actores estatales y no estatales utilizan plataformas tecnológicas, redes sociales, inteligencia artificial y campañas de influencia para modificar comportamientos sociales, manipular narrativas y afectar la estabilidad política de sus adversarios.

Las operaciones de influencia y desinformación representan actualmente una herramienta estratégica de alto impacto. A través de campañas coordinadas, difusión automatizada de contenido, utilización de bots, inteligencia artificial generativa y deepfakes, es posible erosionar la confianza institucional, polarizar sociedades y debilitar la cohesión nacional sin recurrir necesariamente al enfrentamiento militar directo. Como sostienen Singer y Brooking (2018), la batalla por la percepción pública se ha convertido en un componente esencial de los conflictos modernos, donde controlar la narrativa puede resultar tan relevante como controlar el territorio.

Asimismo, la guerra cognitiva busca influir directamente sobre la voluntad y capacidad de decisión de individuos, organizaciones y gobiernos. Esta modalidad de conflicto explota vulnerabilidades psicológicas, emocionales y culturales mediante operaciones persistentes de manipulación informacional, combinando elementos de propaganda, desinformación y guerra psicológica. El objetivo no es únicamente engañar al adversario, sino alterar su capacidad de análisis, generar incertidumbre y debilitar su cohesión social y política (Johnson, 2019).

En este contexto, la defensa nacional deja de ser exclusivamente una cuestión militar para convertirse en un problema sistémico e integral que involucra infraestructura digital, resiliencia social, seguridad económica y gobernanza tecnológica. La protección de infraestructuras críticas, la ciberseguridad nacional, la alfabetización digital de la población y la capacidad estatal para responder a campañas de desinformación pasan a formar parte de las prioridades estratégicas de seguridad.

La transición hacia escenarios multidominio también transforma profundamente la planificación y conducción de operaciones militares. Las fuerzas armadas modernas requieren estructuras más flexibles, interoperables y tecnológicamente integradas, capaces de operar simultáneamente en distintos entornos y responder a amenazas híbridas de alta complejidad. Esto implica desarrollar doctrinas conjuntas, capacidades de inteligencia en tiempo real, automatización de procesos de decisión y mecanismos avanzados de coordinación entre actores militares, civiles y tecnológicos.

El entorno multidominio redefine el concepto mismo de poder estratégico. La capacidad de dominar la información, proteger infraestructuras digitales, garantizar resiliencia tecnológica y mantener superioridad cognitiva se convierte en un factor decisivo para preservar la soberanía nacional y la estabilidad internacional. En consecuencia, los conflictos futuros estarán determinados no solo por la capacidad militar convencional de los Estados, sino por su habilidad para integrar eficazmente tecnología, información, inteligencia y resiliencia en un ecosistema multidominio altamente dinámico y competitivo.

Nuevas Tecnologías Disruptivas

La Inteligencia Artificial militar se aplica a la fusión de sensores, análisis de inteligencia, mantenimiento predictivo, optimización logística y apoyo a la planificación operativa mediante modelos de aprendizaje automático. En particular, la analítica predictiva permite identificar patrones en grandes volúmenes de datos (imágenes, señales, telemetría y fuentes abiertas), mejorando la detección temprana de amenazas y la asignación de recursos bajo incertidumbre (Scharre, 2018). Estas capacidades tienden a desplazar la ventaja hacia quie-

nes controlan datos de calidad, infraestructura computacional y procesos robustos de validación.

Área de Aplicación	Capacidad IA	Impacto Operacional
Fusión de sensores	Análisis predictivo	Detección temprana de amenazas
Inteligencia	Procesamiento de Big Data	Identificación de patrones
Logística	Optimización de recursos	Eficiencia operativa
Mantenimiento	Análisis predictivo	Disponibilidad de equipos
Planificación	Modelado de escenarios	Apoyo a decisiones

Tabla 1. Aplicaciones de la Inteligencia Artificial en Operaciones Militares. Fuente: Elaboración propia basada en Scharre (2018) y NATO (2021).

No obstante, el uso de IA en apoyo a decisiones introduce riesgos de opacidad, sesgos y sobreconfianza en recomendaciones algorítmicas, especialmente cuando los modelos se entrenan con datos incompletos o no representativos. La evidencia en ética de IA sugiere que la trazabilidad, la explicabilidad y la supervisión humana significativa son condiciones necesarias para reducir errores sistemáticos y evitar escaladas no intencionales en contextos de alta presión temporal (Johnson, 2019). Por ello, la integración efectiva requiere gobernanza de datos, pruebas operacionales continuas y criterios doctrinarios claros sobre responsabilidades.

Los sistemas autónomos y los drones han ampliado la persistencia, el alcance y la precisión de la vigilancia y el ataque, reduciendo costos relativos y riesgos para el personal. La evolución hacia enjambres (swarming) —múltiples plataformas coordinadas por algoritmos— promete saturar defensas, distribuir funciones (reconocimiento, interferencia, ataque) y adaptarse dinámicamente a pérdidas o cambios del entorno (Scharre, 2018). En escenarios disputados, la autonomía puede sostener operaciones cuando las comunicaciones son degradadas o intermitentes.

Sin embargo, la autonomía letal plantea dilemas éticos y jurídicos sobre distinción, proporcionalidad y atribución de responsabilidad, especialmente si la selección y el compromiso de objetivos se delegan a sistemas con capacidad de aprendizaje. Diversos análisis advierten que la reducción del “costo político” del uso de la fuerza y la aceleración del ciclo de ataque pueden disminuir los umbrales de escalada y complicar el control civil-militar (Johnson, 2019). En

consecuencia, los marcos normativos y las reglas de enfrentamiento deben incorporar límites verificables, auditorías y mecanismos de rendición de cuentas.

Nivel	Descripción	Control Humano
Nivel 1	Semiautónomo	Supervisión continua
Nivel 2	Autónomo supervisado	Supervisión intermitente
Nivel 3	Autónomo condicional	Intervención bajo condiciones
Nivel 4	Totalmente autónomo	Mínima intervención

Tabla 2. Niveles de Autonomía en Sistemas de Armas. Fuente: Adaptado de U.S. Department of Defense (2020).

Las capacidades de ciberdefensa y ciberataque se han consolidado como componentes esenciales de la estrategia de seguridad y defensa de los Estados modernos. En el contexto de los conflictos contemporáneos, el ciberespacio dejó de ser un simple entorno tecnológico de soporte para convertirse en un dominio operacional estratégico donde se desarrollan acciones ofensivas, defensivas, de espionaje y de influencia con impactos potencialmente equivalentes a los producidos por operaciones militares convencionales. La creciente digitalización de las infraestructuras críticas, de los sistemas de comando y control y de las redes de comunicación ha generado un escenario donde la superioridad cibernética puede determinar la capacidad de un actor para sostener operaciones militares, garantizar estabilidad institucional y preservar la soberanía nacional.

Las operaciones de ciberataque tienen como objetivo degradar, interrumpir, manipular o destruir sistemas de información adversarios mediante técnicas de intrusión y explotación de vulnerabilidades. Estas acciones pueden dirigirse contra objetivos militares, gubernamentales, económicos o sociales, afectando tanto capacidades operacionales como la confianza pública y la estabilidad política. Entre sus finalidades principales se encuentran la exfiltración de información sensible, el sabotaje de infraestructuras críticas, la interrupción de servicios esenciales y la preparación del entorno para operaciones cinéticas posteriores.

La ofensiva cibernética se sustenta en procesos avanzados de reconocimiento, recopilación de inteligencia, explotación de fallas de seguridad y establecimiento de persistencia dentro de redes comprometidas. Los actores ofensivos emplean herramientas sofisticadas como malware avanzado, ransomware, ataques de denegación de servicio distribuido (DDoS), explotación de vulnerabilidades zero-day y campañas de spear phishing altamente dirigidas. Estas capacidades permiten infiltrarse silenciosamente en sistemas críticos y mantener acceso prolongado sin ser detectados, facilitando operaciones de espionaje estratégico o preparación para acciones disruptivas futuras.

Uno de los elementos más relevantes del ciberataque contemporáneo es su capacidad de operar de manera persistente y encubierta por debajo del umbral de guerra convencional. A diferencia de los conflictos tradicionales, donde los enfrentamientos armados suelen tener límites geográficos y temporales más definidos, el ciberespacio constituye un entorno de confrontación continua y permanente. Los Estados y actores patrocinados mantienen campañas sostenidas de reconocimiento, espionaje y acceso estratégico sobre infraestructuras adversarias incluso en tiempos de aparente paz, configurando un escenario de competencia constante y difícilmente delimitable (NATO, 2021).

En contrapartida, la ciberdefensa busca proteger sistemas, redes e infraestructuras frente a amenazas digitales mediante mecanismos preventivos, detectivos y reactivos. Una estrategia efectiva de defensa cibernética requiere implementar modelos integrales de gestión de riesgos, monitoreo continuo, inteligencia de amenazas y capacidad de respuesta rápida ante incidentes. Esto implica desarrollar arquitecturas tecnológicas resilientes capaces de resistir ataques sofisticados y asegurar la continuidad operacional incluso en condiciones de alta degradación.

Entre las capacidades fundamentales de la ciberdefensa se encuentran la gestión permanente de vulnerabilidades, segmentación de redes, autenticación robusta, cifrado de comunicaciones y monitoreo avanzado mediante centros de operaciones de seguridad (SOC) y equipos de respuesta a incidentes (CSIRT). Asimismo, la utilización de inteligencia artificial y analítica avanzada permite detectar patrones anómalos, correlacionar eventos en tiempo real y anticipar comportamientos hostiles antes de que produzcan impactos significativos.

La protección de infraestructuras críticas representa uno de los mayores desafíos de la ciberdefensa moderna. Sectores como energía, telecomunicaciones, transporte, sistemas financieros, salud y abastecimiento de agua dependen crecientemente de sistemas digitales interconectados que pueden convertirse en objetivos prioritarios durante conflictos híbridos. Un ataque exitoso contra estas infraestructuras no solo afecta capacidades militares, sino también la estabilidad económica, la gobernabilidad y la confianza de la población. En consecuencia, la ciberseguridad nacional debe concebirse como un componente transversal de la resiliencia estratégica del Estado.

La complejidad del entorno cibernético se incrementa debido a la dificultad de atribuir con precisión la autoría de los ataques. La naturaleza distribuida y anónima de Internet permite ocultar el origen de las operaciones mediante redes intermedias, infraestructura comprometida y actores proxy. Esta incertidumbre dificulta la aplicación de mecanismos tradicionales de disuasión y respuesta estratégica, ya que los Estados pueden enfrentar ataques significativos sin contar con evidencia concluyente sobre el responsable directo.

Además de actores estatales, participan en el ciberespacio grupos paraestatales, organizaciones criminales, hacktivistas y empresas privadas con capacidades ofensivas avanzadas. Esta multiplicidad de actores genera un entorno híbrido donde las fronteras entre guerra, espionaje, criminalidad y operaciones de influencia se vuelven cada vez más difusas. Algunos Estados utilizan grupos de ciberdelincuencia o colectivos ideológicamente alineados como instrumentos indirectos para ejecutar operaciones de desestabilización con niveles variables de negación plausible.

Los ataques patrocinados por Estados suelen perseguir objetivos estratégicos de largo plazo relacionados con espionaje político, obtención de propiedad intelectual, sabotaje industrial o coerción geopolítica. En muchos casos, estas operaciones se desarrollan de forma silenciosa durante largos períodos, permitiendo acceder a información sensible o posicionarse dentro de infraestructuras críticas para futuras acciones ofensivas. La interconexión global de redes civiles y militares amplifica el impacto potencial de estas operaciones, ya que una vulnerabilidad explotada en un sistema civil puede afectar indirectamente capacidades estratégicas nacionales.

La literatura especializada sostiene que las ciberoperaciones raramente actúan de manera aislada. Por el contrario, suelen integrarse con campañas de desinformación, presión económica, operaciones psicológicas y maniobras diplomáticas, configurando estrategias de guerra híbrida orientadas a debilitar gradualmente al adversario sin desencadenar necesariamente un conflicto militar abierto (Singer & Brookings, 2018; NATO, 2021). Esta combinación de herramientas tecnológicas, informacionales y políticas permite ejercer presión sostenida sobre Estados adversarios mediante acciones ambiguas y difíciles de responder de manera simétrica.

Asimismo, el uso de inteligencia artificial en el ámbito cibernético introduce nuevos desafíos y oportunidades. Los sistemas automatizados permiten acelerar procesos de detección, correlación y respuesta frente a amenazas, pero también pueden ser utilizados ofensivamente para desarrollar malware adaptable, campañas automatizadas de phishing o herramientas de evasión avanzadas. Esta dinámica genera una carrera tecnológica permanente entre capacidades ofensivas y defensivas, donde la velocidad de innovación se convierte en un factor crítico de superioridad estratégica.

En el contexto de los escenarios operacionales futuros, la ciberdefensa ya no puede considerarse únicamente una función técnica de protección informática, sino un componente integral de la seguridad nacional y de la conducción estratégica multidominio. Los Estados deberán desarrollar doctrinas, capacidades humanas y marcos legales capaces de responder a amenazas cada vez más sofisticadas, persistentes y globales. La capacidad de anticipar, resistir y recuperarse de ataques cibernéticos será un elemento determinante para preservar la soberanía, la estabilidad institucional y la continuidad operacional en los conflictos del siglo XXI.

La computación cuántica podría alterar de forma sustantiva la criptografía y, por extensión, la seguridad de comunicaciones militares, al habilitar —en determinados supuestos— la ruptura de esquemas criptográficos ampliamente utilizados. Aunque su madurez operacional aún es limitada, la planificación estratégica debe considerar la transición hacia criptografía poscuántica, así como oportunidades en optimización, simulación y detección que podrían mejorar la planificación y la guerra antisubmarina o espacial (NATO, 2021).

Los sistemas de vigilancia inteligente combinan sensores ubicuos con reconocimiento facial, análisis de comportamiento y detección de anomalías para identificar patrones en entornos urbanos y fronterizos. Estas capacidades pueden mejorar la protección de fuerzas y la seguridad de instalaciones, pero también elevan riesgos de abuso, discriminación algorítmica y erosión de derechos, por lo que requieren controles legales, transparencia y evaluación de impacto (Johnson, 2019).

La guerra electrónica avanzada busca dominar el espectro electromagnético mediante interferencia, engaño, supresión de defensas y protección de enlaces propios. En un entorno saturado de sensores y comunicaciones, la capacidad de degradar radares, navegación y enlaces de datos puede ser decisiva para negar acceso, reducir precisión adversaria y proteger operaciones multidominio. La tendencia apunta a sistemas más adaptativos, apoyados por IA, capaces de identificar emisiones y ajustar técnicas de interferencia en tiempo casi real (Scharre, 2018).

Las operaciones multidominio se orientan a generar efectos coordinados en tierra, mar, aire, espacio, ciberespacio y esfera informacional/cognitiva de manera simultánea, con el fin de crear dilemas al adversario y explotar ventanas de oportunidad. En este enfoque, la ventaja proviene de la integración de inteligencia, fuegos, maniobra y protección en redes distribuidas, donde la información fluye con baja latencia y alta resiliencia (NATO, 2021). La interoperabilidad técnica y doctrinaria se vuelve, por tanto, un requisito estructural.

Dominios	Descripción
Terrestre	Maniobra, control de terreno y protección de fuerzas.
Marítimo	Control de líneas de comunicación, proyección y negación de área.
Aéreo	Superioridad aérea, ISR y fuegos de precisión.
Espacial	Posicionamiento, navegación, comunicaciones y alerta temprana.
Cibernético	Defensa/ofensiva sobre redes, datos y sistemas críticos.
Cognitivo	Influencia sobre percepciones, decisiones y cohesión social.

Tabla 3. Dominios de Operaciones Militares Contemporáneas. Fuente: Elaboración propia basada en NATO (2021).

La coordinación multidominio también incrementa la complejidad del mando y control: más sensores y efectores no garantizan mejores resultados si la arquitectura de decisión no filtra, prioriza y asigna responsabilidades con claridad. La evidencia sugiere que la saturación informacional puede degradar el juicio humano, por lo que se requieren herramientas de apoyo basadas en IA, junto con procedimientos que preserven la comprensión contextual y eviten automatismos peligrosos (Johnson, 2019). En síntesis, la integración debe equilibrar velocidad con control y legitimidad.

La guerra híbrida combina tácticas convencionales con acciones irregulares, coerción económica, operaciones de información y ciberataques para alcanzar objetivos políticos sin recurrir necesariamente a una guerra declarada. Este enfoque explota ambigüedades legales y narrativas, buscando fragmentar alianzas, erosionar la confianza pública y limitar la capacidad de respuesta del Estado objetivo (Singer & Brooking, 2018). La hibridación se potencia con tecnologías de bajo costo y alta difusión, como drones comerciales adaptados y herramientas automatizadas de propaganda.

Para la defensa, el desafío radica en que los vectores híbridos operan de forma persistente y distribuida, afectando simultáneamente seguridad interior, defensa exterior y estabilidad institucional. La respuesta requiere coordinación interagencial, marcos de atribución y umbrales de respuesta, así como capacidades de resiliencia social y protección de infraestructura digital. En términos doctrinarios, la preparación debe contemplar escenarios "zona gris" donde la disuasión tradicional es menos efectiva y la escalada puede ser gradual (NATO, 2021).

La guerra cognitiva se centra en influir sobre cómo las audiencias perciben la realidad, evalúan riesgos y toman decisiones, utilizando operaciones psicológicas, propaganda, microsegmentación y manipulación de agendas. En ecosistemas mediáticos algorítmicos, la amplificación de contenidos polarizantes y la explotación de sesgos cognitivos pueden producir efectos estratégicos desproporcionados respecto del costo de la operación (Singer & Brooking, 2018). Así, la superioridad informacional se convierte en un componente de la superioridad militar.

La influencia digital se apoya crecientemente en automatización: bots, granjas de contenido y sistemas de recomendación adversarios que optimizan mensa-

jes para maximizar alcance y credibilidad aparente. La literatura sugiere que la defensa efectiva exige alfabetización mediática, transparencia de plataformas, capacidades de detección de campañas coordinadas y comunicación estratégica coherente, además de marcos legales que protejan libertades sin dejar vacíos explotables (Johnson, 2019; NATO, 2021). En este dominio, la resiliencia social es tan relevante como la ciberseguridad técnica.

Vector de Ataque	Mecanismo	Contramedida
Desinformación	Narrativas falsas	Verificación y fact-checking
Deepfakes	Medios sintéticos	Detección forense
Microsegmentación	Algoritmos de targeting	Transparencia de plataformas
Amplificación automatizada	Bots y trolls	Detección de comportamiento anómalo
Manipulación psicológica	Explotación de sesgos	Alfabetización mediática

Tabla 4. Vectores de Guerra Cognitiva y Contramedidas. Fuente: Elaboración propia basada en Singer, P. W., & Brooking, E. T. (2018).

La automatización de decisiones mediante IA promete acelerar el ciclo OODA (observar–orientar–decidir–actuar) al priorizar información, sugerir cursos de acción y asignar recursos en tiempo real. En operaciones de alta velocidad —por ejemplo, defensa aérea, ciberdefensa o guerra electrónica— la reducción de latencia puede ser determinante para sobrevivir y mantener iniciativa. Sin embargo, el incremento del tempo operacional también puede comprimir el tiempo disponible para deliberación humana y control político, elevando el riesgo de errores y escaladas no deseadas (Johnson, 2019).

El human-machine teaming (integración humanomáquina) requiere definir qué decisiones pueden automatizarse, cuáles deben permanecer bajo control humano y cómo se auditan los sistemas en condiciones reales. La evidencia sugiere que la confianza calibrada —ni ciega ni escéptica— depende de entrenamiento, explicabilidad y procedimientos de contingencia cuando los modelos fallan o son degradados por el adversario (Scharre, 2018). En términos estratégicos, la automatización debe acompañarse de gobernanza, pruebas de robustez y reglas de empleo que preserven responsabilidad y legitimidad.

Riesgos y Amenazas Futuras

Dependencia tecnológica

La dependencia excesiva de tecnologías conectadas puede generar vulnerabilidades sistémicas: fallas de software, interrupciones de comunicaciones, degradación por interferencia o ataques a la cadena de suministro pueden paralizar capacidades críticas. En entornos disputados, la resiliencia exige redundancia, modos degradados de operación y entrenamiento para continuar misiones con información incompleta. La planificación debe asumir que la conectividad no es garantizada y que el adversario buscará atacar los “nervios” digitales antes que las plataformas (NATO, 2021).

Vulnerabilidades de IA

Los sistemas de IA son susceptibles a ataques adversarios, manipulación de entradas, envenenamiento de datos y extracción de modelos, lo que puede inducir clasificaciones erróneas o decisiones subóptimas. En contextos militares, estas vulnerabilidades pueden traducirse en identificación incorrecta de objetivos, falsas alarmas o degradación de la conciencia situacional. Por ello, se requieren prácticas de seguridad de IA, validación continua, control de datos y pruebas frente a adversarios realistas (Johnson, 2019).

Deepfakes y desinformación

Los deepfakes y otros medios sintéticos permiten fabricar audio, video e imágenes con alta verosimilitud, erosionando la confianza en evidencias y acelerando la difusión de narrativas falsas. En crisis, la circulación de material manipulado puede provocar pánico, deslegitimar autoridades o desencadenar respuestas precipitadas, especialmente cuando se combina con microsegmentación y amplificación automatizada (Singer & Brooking, 2018). La amenaza no es solo la falsificación, sino la “negación plausible” que dificulta establecer hechos compartidos.

Las contramedidas incluyen capacidades técnicas de detección, verificación forense, trazabilidad de contenidos y protocolos de comunicación pública para

desmentidos rápidos y creíbles. Sin embargo, la literatura advierte que la respuesta puramente técnica es insuficiente si no se acompaña de confianza institucional, coordinación con plataformas y educación mediática sostenida (Johnson, 2019; NATO, 2021). En términos operacionales, la gestión de la información debe integrarse a la planificación desde el inicio, no como actividad reactiva.

Ataques a infraestructuras críticas

Los ataques a infraestructuras críticas —energía, agua, transporte, salud, finanzas y telecomunicaciones— pueden generar efectos estratégicos al afectar la continuidad del Estado y la capacidad de sostener operaciones militares. La interdependencia entre sistemas industriales y redes digitales amplía la superficie de ataque y facilita operaciones de sabotaje o coerción por debajo del umbral cinético. En este marco, la defensa requiere segmentación, monitoreo industrial, ejercicios de continuidad y coordinación públicoprivada (NATO, 2021).

Sector	Vulnerabilidad Principal	Impacto Potencial
Energía	Sistemas SCADA	Apagones masivos
Telecomunicaciones	Redes de datos	Pérdida de comunicaciones
Transporte	Sistemas de control	Paralización logística
Salud	Registros médicos	Colapso sanitario
Finanzas	Sistemas de pago	Crisis económica
Agua	Sistemas de tratamiento	Contaminación o desabastecimiento

Tabla 5. Infraestructuras Críticas Vulnerables a Ciberataques. Fuente: Elaboración propia basada en NATO (2021).

Un riesgo central es el de fallas en cascada: la interrupción de un sector puede degradar múltiples servicios esenciales, amplificando el impacto social y político. La planificación de resiliencia debe incorporar análisis de dependencias, reservas estratégicas, capacidades de recuperación rápida y mecanismos de mando unificado para crisis complejas. La evidencia sugiere que la preparación previa —incluidos simulacros y acuerdos de intercambio de información— reduce significativamente el tiempo de restauración y la incertidumbre decisional (NATO, 2021).

Impacto Estratégico Nacional

Necesidad de capacidades nacionales de ciberdefensa

El desarrollo de capacidades nacionales de ciberdefensa es un imperativo para proteger redes gubernamentales, sistemas militares y servicios esenciales (públicos o privados) frente a amenazas persistentes. Esto implica establecer centros de operaciones de seguridad, equipos de respuesta a incidentes, marcos de gestión de riesgos y estándares mínimos para proveedores críticos. La experiencia comparada sugiere que la eficacia aumenta cuando existe coordinación interinstitucional, intercambio de inteligencia y ejercicios conjuntos que simulan ataques complejos (NATO, 2021).

Además, la ciberdefensa debe integrarse con doctrina de disuasión y respuesta, considerando opciones diplomáticas, legales y, cuando corresponda, capacidades ofensivas bajo control político. La integración con operaciones de información y protección de infraestructura crítica permite abordar campañas híbridas de manera coherente. En términos de gobernanza, resulta clave definir responsabilidades, umbrales de escalada y mecanismos de atribución que sostengan legitimidad interna y externa (Johnson, 2019; NATO, 2021).

Formación de talento especializado

La formación de talento especializado en IA, ciencia de datos, ciberseguridad, ingeniería de sistemas y ética tecnológica es un factor habilitante para la transformación militar. Programas de carrera, alianzas con universidades, laboratorios de innovación y rutas de certificación pueden reducir brechas de capacidades y mejorar la retención. La evidencia sugiere que equipos multidisciplinarios —operadores, ingenieros, juristas y analistas— incrementan la calidad de adopción tecnológica y disminuyen riesgos de implementación (Scharre, 2018).

En términos estratégicos, la formación de capital humano especializado se convierte en un multiplicador de poder nacional. La capacidad de desarrollar, adaptar y operar tecnologías críticas dependerá cada vez más del conocimiento y de la preparación de los recursos humanos disponibles. Los Estados que logren construir ecosistemas sólidos de formación, innovación y retención de talento estarán mejor posicionados para enfrentar desafíos multidominio, pro-

teger su soberanía tecnológica y garantizar resiliencia frente a amenazas emergentes.

En los escenarios operacionales futuros, la superioridad tecnológica no estará determinada únicamente por la adquisición de equipamiento avanzado, sino por la capacidad de formar personas capaces de comprender, integrar y evolucionar dichas tecnologías dentro de estructuras estratégicas eficientes y resilientes. El talento humano continuará siendo el componente decisivo para transformar innovación tecnológica en capacidad operacional efectiva y sostenida en el tiempo.

Cooperación internacional

La cooperación internacional facilita interoperabilidad, intercambio de inteligencia, estándares comunes y aprendizaje de lecciones operacionales, especialmente en ciberdefensa y lucha contra desinformación. En alianzas y marcos multilaterales, la coordinación permite responder a amenazas transnacionales y reducir asimetrías tecnológicas mediante proyectos conjuntos y ejercicios combinados (NATO, 2021). No obstante, requiere equilibrar soberanía, protección de datos y seguridad de la información compartida.

Desarrollo doctrinario y normativo

La incorporación de IA, autonomía y operaciones multidominio exige actualizar doctrina para definir conceptos de empleo, estructuras de mando, reglas de enfrentamiento y criterios de evaluación de efectos. La doctrina debe especificar niveles de autonomía, condiciones de supervisión humana y procedimientos de verificación, así como integrar ciberoperaciones e influencia informacional en la planificación conjunta. La literatura sugiere que la doctrina efectiva traduce capacidades técnicas en ventajas operacionales reproducibles mediante entrenamiento y estandarización (Freedman, 2017; Scharre, 2018).

En paralelo, los marcos normativos deben abordar responsabilidad, transparencia y cumplimiento del derecho internacional humanitario, especialmente ante sistemas que recomiendan o ejecutan acciones con mínima intervención humana. La ética aplicada a la guerra automatizada demanda criterios de con-

trol, auditabilidad y proporcionalidad, además de mecanismos de revisión y rendición de cuentas. En términos estratégicos, la legitimidad se convierte en un multiplicador de poder: sin ella, la superioridad tecnológica puede generar costos políticos y operacionales que neutralicen sus beneficios (Johnson, 2019).

La necesidad de integrar tecnología, doctrina y factor humano

La transformación del poder militar en la era de la IA requiere integrar tecnología, doctrina y factor humano en un mismo diseño de fuerza. La automatización puede aumentar el tempo y la eficacia, pero también introduce nuevas superficies de ataque, sesgos y riesgos de escalada; por ello, la supervisión humana significativa, la gobernanza de datos y la seguridad de IA deben considerarse requisitos operacionales, no añadidos posteriores (Johnson, 2019). La preparación debe incluir entrenamiento para operar en condiciones degradadas y para evaluar críticamente recomendaciones algorítmicas.

Finalmente, la adaptación institucional demanda inversión sostenida en talento, investigación, alianzas y marcos normativos que preserven legitimidad y control democrático. En escenarios multidominio y cognitivos, la eficacia militar dependerá tanto de la protección de infraestructuras críticas y la resiliencia social como de la modernización de plataformas. La evidencia disponible sugiere que quienes logren articular innovación tecnológica con doctrina flexible y liderazgo competente estarán mejor posicionados para enfrentar conflictos híbridos, persistentes y altamente automatizados (Singer & Brooking, 2018; NATO, 2021).

La Prospectiva Estratégica

Para ver los escenarios futuros, se utiliza la prospectiva estratégica como herramienta analítica. Basado en los postulados de Godet y Durance (2011), en el cual la prospectiva no busca predecir el futuro de manera determinista, sino reducir la incertidumbre mediante la identificación de tendencias, variables clave y señales débiles en el presente.

Para el presente artículo, el análisis se despliega sobre dos horizontes temporales definidos: Mediano Plazo (Horizonte 2030) teniendo enfoque centrado en

las trayectorias de transición doctrinal, la interoperabilidad de sistemas actuales y la adopción inicial de capacidades automatizadas en las fuerzas armadas; y Largo Plazo (Horizonte 2035-2040) con el enfoque de carácter disruptivo, donde se evalúa la maduración de la autonomía total en combate, la guerra algorítmica generalizada y la dilución definitiva de las fronteras físicas en el entorno multidominio.

Arquitecturas Tecnológicas y Procesamiento Multidominio

Para comprender la complejidad operativa en los escenarios futuros, es imperativo analizar cómo se estructuran las plataformas de defensa y cómo se procesa el flujo de información estratégica. La integración de sistemas avanzados se sustenta en dos dimensiones críticas: la automatización de la defensa física conjunta y la resiliencia cognitiva en el procesamiento de la información.

Interoperabilidad de Sistemas de Armas y Datos: El Modelo de Mando y Control

Wogalter (2006), afirma que para que una operación dentro del entorno multidominio sea exitosa, depende de arquitecturas tecnológicas capaces de integrar sensores distribuidos y efectores tácticos bajo un núcleo centralizado de procesamiento algorítmico. Un ejemplo histórico y vigente de esta integración sistémica es el esquema de un sistema de combate integrado naval de alta complejidad, conceptualizado doctrinalmente a partir de las arquitecturas de defensa aérea y antimisiles de área.

Como se aprecia en las arquitecturas complejas de defensa (Figura 1), el núcleo operativo se compone de un Sistema de Mando y Decisión (Command and Decision System) interconectado de manera síncrona con un Sistema de Control de Armas (Weapon Control System). Este ecosistema integra de forma transversal múltiples sensores y vectores cómo son: Sensores de Detección Multidominio: Sistemas de Sonar (submarino), Radar ADT y el Radar principal de escaneo de fase activa (como el AN/SPY-1A), sistemas de navegación y subsistemas de detección electrónica (guerra electrónica); Enlaces de Datos Tácticos (Tactical Data Links): Canales automatizados como el Link 11, Link 14 y Link 4A, que operan como el tejido de comunicaciones que viabiliza la interoperabi-

lidad conjunta y Sistemas de Armas y Efectores: Plataformas que ejecutan la respuesta cinética o táctica, incluyendo aeronaves (Seahawk), misiles de crucero de largo alcance (Tomahawk), misiles antibuque (Harpoon), defensas de punto de corto alcance (Phalanx) y control de fuego de artillería.

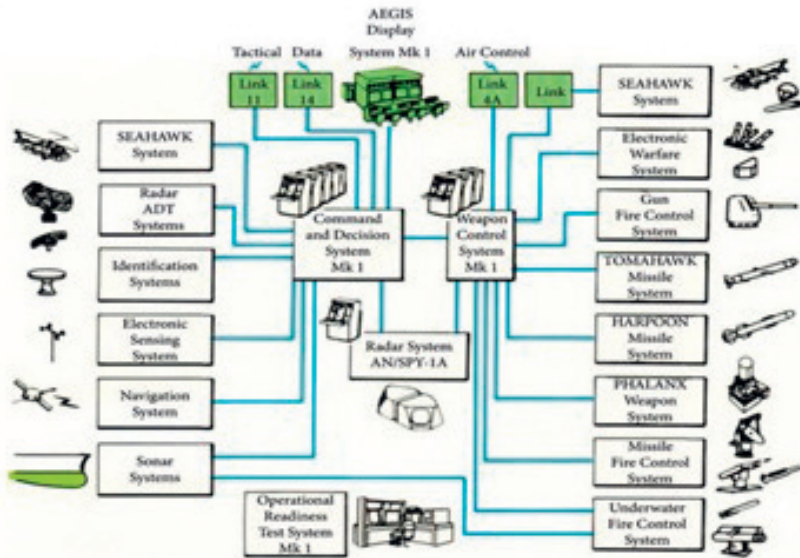


Figura 1. Aegis Combat System Display - J. Li et al (2010).

En los escenarios futuros, la incorporación de la Inteligencia Artificial en estos sistemas embebidos no reemplaza la estructura de mando, sino que automatiza la fusión de datos de los sensores, acelerando la asignación de armas ante amenazas saturantes a velocidades que superan la capacidad de cómputo puramente humana.

El Factor Humano y la Dimensión Cognitiva en el Procesamiento del Mensaje

Cómo señala Cranor (2008), el flujo de información masiva que un entorno tecnológico multidominio inyecta en los puestos de mando genera un desafío crítico en el receptor humano (Comando).

Para que la información de inteligencia se traduzca en una decisión táctica eficiente (Comportamiento o Behavior), debe atravesar un proceso cognitivo secuencial que se ve constantemente amenazado por variables ambientales y operativas.

El modelo de procesamiento del receptor humano (Figura 2) demuestra que la "Comunicación" (u órdenes doctrinales en el campo de batalla) debe superar primero los Impedimentos de la Comunicación, clasificados estos en Estímulos Ambientales e Interferencias. En un entorno de combate contemporáneo, estas interferencias equivalen a las acciones de guerra electrónica (jamming), ciberoperaciones de desinformación o la simple niebla de la guerra física. Una vez que el flujo informativo penetra las barreras ambientales, es procesado por el Receptor Humano (Comando) bajo tres dimensiones analíticas:

1. **Filtros Internos y Capacidades:** Las Variables Personales (demografía, características personales, conocimiento y experiencia previa) interactúan con las Intenciones (actitudes, creencias y motivación) y las Capacidades individuales del operador o comandante.
2. **Distribución y Procesamiento de la Comunicación:** El flujo cognitivo requiere una conmutación de la atención y el mantenimiento de la misma, esenciales para alcanzar la Comprensión y la Adquisición de Conocimiento sobre la amenaza detectada.
3. **Aplicación:** El ciclo culmina con la retención del conocimiento y la transferencia de este hacia las unidades subordinadas.

Este modelo cognitivo fundamenta por qué el desarrollo de interfaces de Inteligencia Artificial debe diseñarse específicamente para mitigar la sobrecarga cognitiva del operador militar, reduciendo la interferencia y optimizando la velocidad de comprensión para asegurar una respuesta táctica o comportamiento operacional preciso ante las amenazas en el ciberespacio y el plano físico.

El Desafío de la Interoperabilidad Concurrente y la Fusión de Datos

La discusión en torno a sistemas complejos de mando y control (análogos a las arquitecturas como el sistema AEGIS analizado) revela que a corto plazo el factor determinante no será la velocidad del vector cinético (el misil o la aeronave), sino la interoperabilidad de los enlaces de datos tácticos (Tactical Data

Links). Los teatros de operaciones futuros exigen que los flujos informáticos de sensores submarinos, radares de barrido activo terrestres y satélites de observación espacial converjan en sistemas de Mando y Decisión unificados.

La influencia de la Inteligencia Artificial Estrecha (ANI) se centraría en la fusión de datos de sensores. El análisis documental denota que los algoritmos de aprendizaje profundo se utilizarán para limpiar el “ruido” electromagnético y clasificar blancos de manera automática, reduciendo la ventana temporal del ciclo de decisión táctica.

Mitigación de la Interferencias y Protección del Receptor Humano

Al contrastar los requerimientos de las Operaciones Multidominio con el modelo cognitivo del Human Receiver (Figura 2), se evidencia una vulnerabilidad crítica en el corto plazo: la sobrecarga de información. La proliferación de estímulos ambientales digitales en un puesto de mando interconectado puede colapsar la capacidad de retención y transferencia de conocimiento del comandante humano y por consiguiente, la discusión científica contemporánea subraya que las ciberoperaciones aliadas a mediano plazo no solo buscarán degradar las redes del adversario, sino asegurar la resiliencia de los canales propios de comunicación mediante técnicas de ciberdefensa activa, asegurando que el proceso de conmutación y mantenimiento de la atención del operador no sea sabotado por operaciones de desinformación o denegación de servicio (DCO).

Horizonte a Largo Plazo: La Disrupción de la Guerra Algorítmica Generalizada y el Combate Autónomo

Una vez que dejemos atrás la fase de transición, el horizonte a largo plazo plantea un escenario donde las tecnologías emergentes alteran la naturaleza ontológica de la maniobra militar.

Autonomía Total y Ecosistemas Crewed-Uncrewed Teaming (CUC-T)

Para el largo plazo, las operaciones basadas en plataformas individuales tripuladas serán obsoletas frente a la consolidación de los sistemas autónomos en

red. Bajo el concepto analizado de Crewed-Uncrewed Teaming (CUC-T), los escenarios de operaciones futuros desplegarán enjambres masivos de vehículos no tripulados (aéreos, terrestres y navales) que coordinarán sus acciones de manera descentralizada mediante IA nativa (Incluso actualmente ya son utilizados estos esquemas en presentaciones turísticas en drones).

La discusión estratégica indica que el rol humano se desplazará definitivamente de la ejecución táctica ("human-in-the-loop") hacia la supervisión de la misión ("human-on-the-loop"). Los enjambres autónomos saturarán los sistemas defensivos convencionales mediante ataques cinéticos y electromagnéticos simultáneos, transformando el principio fundamental de la masa y la concentración de fuerzas.

La Velocidad del Software como Vector Estratégico

En este horizonte de largo plazo, el dominio del ciberespacio y el dominio cognitivo se fusionan por completo debido a la guerra algorítmica. La velocidad de las operaciones ofensivas en el ciberespacio (OCO), potenciadas por IA generativa y computación avanzada, superará de forma absoluta el tiempo de reacción biológica del cerebro humano.

El comportamiento operativo (Behavior) de las unidades de defensa dependerá de la confianza en la autonomía de respuesta de sus propios sistemas informáticos de combate. El riesgo estratégico identificado en este punto es el surgimiento de crisis de escalada imprevistas, donde algoritmos de defensa contra algoritmos de ataque interactúen de manera autónoma en fracciones de segundo, obligando a los marcos doctrinales institucionales a redefinir por completo el concepto de responsabilidad jurídica y ética en el uso de la fuerza.

Panorama General de la Transformación Tecnológica y la Revolución en los Asuntos Militares (RAM)

La velocidad del cambio tecnológico contemporáneo ha superado las transiciones históricas lineales, consolidando una nueva Revolución en los Asuntos Militares (RAM). Bajo este paradigma, la Inteligencia Artificial no se define meramente como una tecnología disruptiva aislada, sino como un elemento con un

impacto potencialmente revolucionario sobre el poder militar, la competencia estratégica global y la política internacional (Horowitz, 2018). Su introducción actúa de manera transversal, alterando las métricas tradicionales con las que las naciones miden su capacidad de disuasión y proyección de fuerza.

Esta transformación se evidencia de manera pragmática en una transición conceptual y operativa: el paso de la simple mejora de equipos hacia el reemplazo de funciones humanas. Mientras que las revoluciones tecnológicas previas optimizaban el armamento existente - haciendo los misiles más rápidos o los blindajes más resistentes -, la convergencia de la IA y los sistemas autónomos viabiliza la sustitución parcial o total de los roles humanos por sistemas inteligentes. Este cambio de paradigma no solo modifica los procedimientos tácticos en el terreno físico, sino que reconfigura profundamente los procesos de razonamiento, la gestión de crisis y la toma de decisiones en contextos de conflicto multidominio.

Desafíos Estratégicos, Éticos y de Estabilidad del Entorno Tecnológico

La adopción de estas capacidades avanzadas no está exenta de fricciones estratégicas. El análisis prospectivo documental permite identificar tres dimensiones críticas de vulnerabilidad:

- *Riesgos de Inestabilidad y Escalada Inadvertida*

La difusión transnacional y acelerada de la IA y las ciberarmas introduce un factor de impredecibilidad en la arquitectura de seguridad global, exacerbando la rivalidad entre grandes potencias. A diferencia de las capacidades nucleares tradicionales, cuyas métricas de disuasión son visibles y verificables, las capacidades algorítmicas y de ciberoperaciones ofensivas (OCO) operan en la opacidad.

Esta falta de transparencia incrementa el riesgo de rutas de escalada inadvertida en escenarios de crisis. Un ejemplo crítico de este fenómeno se observa en la dinámica de competencia entre los Estados Unidos y China dentro del ciberespacio: un ciberataque automatizado mediante IA dirigido a redes de mando y control, diseñado originalmente con fines de contra-inteligencia o degradación táctica limitada, puede ser malinterpretado por los sistemas de alerta temprana del adversario como el preludio de un

ataque estratégico cinético, desencadenando una respuesta desproporcionada fuera del dominio virtual.

– *Dilemas de Ética y Control Humano de la Fuerza*

La automatización de la letalidad a través de los sistemas de armas autónomos (AWS) y las decisiones algorítmicas de control de fuego (análogas al procesamiento automatizado de sistemas complejos de defensa) plantean dilemas éticos y jurídicos de primer orden. La transferencia de la autorización del uso de la fuerza a un algoritmo informático erosiona el principio de responsabilidad y rendición de cuentas bajo el Derecho Internacional Humanitario (DIH).

La incapacidad intrínseca de una IA para procesar el principio de proporcionalidad y distinción en el terreno de combate eleva exponencialmente el riesgo de bajas y víctimas civiles involuntarias. La pérdida del control humano significativo sobre la fuerza empleada altera la esencia de la gobernanza de la defensa, convirtiendo la gestión del combate en un proceso matemático desprovisto de prudencia estratégica.

– *Brechas Normativas y Doctrinales Internacionales*

Existe una asimetría crítica entre la velocidad del desarrollo tecnológico y la capacidad de adaptación institucional. El derecho internacional y las doctrinas de defensa vigentes van muy por detrás de la realidad tecnológica que imponen las ciberoperaciones y los enjambres autónomos. Los vacíos normativos respecto a qué constituye un “ataque armado” en el ciberespacio, o cómo regular la proliferación de software militar de código abierto, generan zonas grises que son explotadas asimétricamente por actores estatales y no estatales, amenazando la estabilidad institucional.

Operaciones en Entorno Multidominio y Ventaja Decisiva

Frente a este panorama, el futuro campo de batalla se concibe definitivamente como un entorno multidominio altamente integrado. Las dimensiones tradicionales - tierra, mar y aire - operan en sincronía absoluta con el espacio exterior y el ciberespacio, cohesionadas mediante redes avanzadas de transmisión de datos tácticos y sistemas de Mando y Control (C2) fuertemente apoyados por estructuras de IA.

Bajo esta arquitectura conceptual, el objetivo central de las fuerzas estratégicas ya no es la simple destrucción física del oponente, sino la obtención de la ventaja decisiva. Esta ventaja se define como la capacidad de procesar la información, comprender el entorno operativo y ejecutar decisiones válidas de manera más rápida y precisa que el adversario. Al explotar de forma combinada las sinergias cruzadas entre dominios (por ejemplo, utilizando una ciberoperación ofensiva para cegar los radares enemigos, facilitando el despliegue de enjambres autónomos aéreos), se logra crear múltiples dilemas simultáneos al oponente. Esta saturación cognitiva y operativa degrada la voluntad de combate del adversario, neutralizando su capacidad de respuesta y logrando, en última instancia, el fin primordial de la política de defensa: la disuasión efectiva de la agresión.

Propuestas Estratégicas e Institucionales

Ante el panorama prospectivo descrito, y con el fin de que las instituciones de defensa del ámbito iberoamericano mantengan su relevancia, resiliencia y capacidades operativas, se elevan las siguientes recomendaciones estratégicas:

1. **Actualización Doctrinal y Normativa de Carácter Flexible:** Las instituciones de defensa deben migrar de manuales de operaciones conjuntos rígidos hacia doctrinas nativas multidominio. Es imperativo diseñar marcos conceptuales que asuman el ciberespacio y el espectro electromagnético no como áreas de apoyo técnico, sino como dominios de maniobra formal. Asimismo, se debe liderar a nivel regional la discusión de marcos jurídicos y éticos que regulen y auditen el uso de algoritmos en los sistemas de defensa, garantizando el estricto cumplimiento del Derecho Internacional Humanitario.
2. **Rediseño de los Perfiles de Liderazgo y Capacitación Cognitiva:** Dado que el factor humano enfrenta un riesgo crítico de saturación y sobrecarga informativa ante el flujo masivo de datos tácticos, los centros de educación superior militar y estratégica deben reconfigurar sus planes de estudio. Se propone: Incentivar la formación en competencias de guerra algorítmica (Ciberguerra), ciberdefensa y analítica de datos, entrenar a los futuros comandantes en entornos híbridos (Human-AI Teaming), capacitando al deci-

sor estratégico para interactuar con sistemas inteligentes sin perder el juicio ético ni la prudencia operativa.

3. Inversión en Resiliencia Digital e Infraestructuras Críticas C2: Para absorber el impacto de las ciberoperaciones ofensivas (OCO) enemigas a mediano y largo plazo, los Estados deben priorizar la inversión en Ciberdefensa Activa (DCO). Esto implica blindar las arquitecturas de Mando y Control, asegurar la redundancia de los enlaces de datos tácticos y garantizar la protección de los sistemas de navegación frente a acciones de guerra electrónica. La resiliencia de la red propia es la condición sine qua non para poder proyectar cualquier tipo de fuerza en el futuro.
4. Fomento de la Autonomía Tecnológica Regional e Interoperabilidad: Se sugiere, además, promover alianzas estratégicas y de cooperación científica entre los países iberoamericanos para el desarrollo compartido de tecnologías de software, sensores y sistemas no tripulados de código abierto. Reducir la dependencia tecnológica de proveedores externos en áreas críticas como la IA aplicada a la defensa es un imperativo de seguridad nacional para salvaguarda de la soberanía institucional.

Finalmente, esto nos permite esgrimir la siguiente pregunta: ¿Oportunidad o Amenaza? El Dilema Estratégico de la Defensa Futura.

Realizado el análisis de la profunda metamorfosis que la Inteligencia Artificial, los sistemas autónomos y las ciberoperaciones imponen sobre el entorno multidominio, la comunidad estratégica global se enfrenta a una pregunta ineludible: la disrupción tecnológica en los escenarios futuros, ¿constituye una oportunidad sin precedentes o una amenaza existencial para la seguridad institucional?

La respuesta a este interrogante no es binaria, sino dialéctica. La tecnología, en su esencia ontológica, es un catalizador que amplifica tanto las virtudes como las vulnerabilidades de los modelos de defensa vigentes.

El Imperativo de la Gobernanza Humana

Podemos afirmar que la influencia de las nuevas tecnologías es una oportunidad o una amenaza depende exclusivamente de la capacidad de anticipación estratégica de las instituciones de seguridad y defensa. La tecnología no posee

una agenda moral propia; su impacto es el reflejo directo de la doctrina que la regula y de la mente del comandante que la orienta.

Para el ámbito de los Colegios de Defensa Iberoamericanos, el desafío no radica en rechazar la evolución tecnológica por temor a sus riesgos, ni en adoptarla ciegamente fascinados por su modernidad. El imperativo estratégico consiste en asumir el liderazgo de esta transformación, blindando las arquitecturas digitales con ciberdefensa activa, adaptando las academias para mitigar las interferencias cognitivas en nuestros decisores, y asegurando - por encima de cualquier velocidad de software - que el control humano significativo permanezca inalterable en el núcleo de la decisión estratégica. Solo bajo esta premisa, la revolución tecnológica dejará de ser una amenaza de exclusión y se convertirá en la mayor oportunidad para garantizar la soberanía, la resiliencia y la paz institucional en los escenarios del futuro.

La Revolución en los Asuntos Militares (RAM) y la Disrupción Digital

El concepto de Revolución en los Asuntos Militares (RAM) describe una transformación profunda en las doctrinas, estructuras organizativas y tecnologías tácticas que altera la conducción de los conflictos bélicos. A diferencia de las RAM del pasado (como la mecanización en el periodo de entreguerras o el desarrollo de las armas nucleares), la RAM digital contemporánea está impulsada casi exclusivamente por el sector civil transnacional y no por laboratorios militares estatales. Como señala la Comisión Económica para América Latina y el Caribe (CEPAL, 2021), la revolución digital en curso está fundamentada en la convergencia de tecnologías que transforman no solo las matrices productivas industriales, sino los mecanismos estatales de seguridad y control territorial. La asimetría tecnológica se convierte así en un vector de vulnerabilidad geopolítica para las naciones de ingresos medios y bajos.

La Interdependencia Compleja y la Erosión del Enclave Territorial

Desde la perspectiva de las Relaciones Internacionales, las dinámicas operativas actuales no pueden explicarse bajo el prisma del realismo político estricto o el aislamiento geográfico. El concepto de "Interdependencia Compleja", pro-

puesto por Robert Keohane y Joseph Nye, explica que los Estados operan en redes densas donde las fronteras son permeables a vectores no estatales y flujos informacionales constantes. Las tecnologías de digitalización masiva y la interconexión global provocan una “perforación” del tejido institucional del Estado, reduciendo su capacidad de aislamiento y obligándolo a redefinir su soberanía operativa (Sassen, 2007). En los escenarios futuros, un ciberataque originado a miles de kilómetros puede paralizar la infraestructura hídrica o energética de un país sin necesidad de que un solo soldado enemigo cruce sus fronteras físicas, desdibujando la línea divisoria tradicional entre el estado de guerra y el de paz.

Las Operaciones Multi-Dominio (MDO)

La doctrina de Operaciones Multi-Dominio representa la respuesta institucional y militar a este entorno interconectado. Desarrollada inicialmente por los centros de pensamiento estratégico globales y ampliamente documentada en los estudios del Centro de Estudios de las Fuerzas Armadas (CEFADIGITAL), la doctrina MDO postula que las fuerzas militares del futuro deben poseer la capacidad de operar de forma simultánea e interconectada a través de cinco dominios clave: tierra, mar, aire, espacio exterior y ciberespacio. La tecnología actúa como el tejido conectivo que unifica estos dominios mediante una “nube de combate” (Combat Cloud) de alta velocidad, donde los sensores distribuidos en satélites, plataformas autónomas marítimas y soldados en tierra alimentan un flujo de datos centralizado y optimizado por algoritmos predictivos.

Análisis Multidimensional de las Tecnologías en el Teatro Operativo Futuro

La reconfiguración de los escenarios de operaciones futuros está dictada por vectores tecnológicos específicos que interactúan de forma sinérgica, potenciando exponencialmente sus efectos en el terreno de combate.

Inteligencia Artificial y la Algoritmización del Mando y Control

La Inteligencia Artificial no representa meramente un incremento marginal en la eficiencia del equipamiento militar, sino el reemplazo progresivo de la capacidad analítica humana en entornos de alta saturación de información. Los sistemas tácticos del futuro dependen del procesamiento en tiempo real de volúmenes masivos de datos desestructurados (Big Data), provenientes de imágenes satelitales, interceptaciones electromagnéticas y sensores biométricos en el frente de batalla.

Los algoritmos de aprendizaje profundo (Deep Learning) permiten el desarrollo del mantenimiento predictivo en plataformas logísticas y la automatización del proceso de selección de objetivos (Targeting). El principal riesgo operacional reside en lo que los analistas militares denominan la “Hiper velocidad de la Guerra” (Hyperwar), un escenario donde la velocidad del combate algorítmico supera la capacidad cognitiva de procesamiento de un operador humano. En consecuencia, las jerarquías de mando se ven forzadas a delegar facultades críticas de decisión a sistemas autónomos, reduciendo el margen de supervisión humana activa y trasladando la toma de decisiones al software de combate.

Sistemas Autónomos Letales (LAWS) y la Guerra de Enjambres

El despliegue de Sistemas Armados Autónomos Letales (LAWS, por sus siglas en inglés) representa una ruptura ética e instrumental definitiva en la historia de los conflictos armados. Los drones modernos ya no operan únicamente bajo la modalidad de control remoto (Man-in-the-loop); las nuevas arquitecturas de software permiten la autonomía de navegación y ejecución de fuego (Man-out-of-the-loop).

La manifestación más avanzada de esta tecnología es el empleo de enjambres de drones autónomos (Swarms). Inspirados en comportamientos biológicos colectivos, estos enjambres coordinan de forma descentralizada sus trayectorias de vuelo mediante redes de comunicación local interconectadas. Si una unidad es derribada por contramedidas enemigas, el enjambre se reconfigura de manera autónoma en milisegundos para cumplir la misión original. Esta táctica neutraliza la efectividad de los sistemas de defensa antiaérea tradicionales

(diseñados para interceptar objetivos unitarios de alto costo, como misiles o aeronaves tripuladas), saturando las redes de defensa del adversario mediante plataformas de bajo costo económico de producción masiva.

El Ciberespacio y el Espectro Electromagnético como Vectores Dominantes

El ciberespacio ha dejado de ser una dimensión puramente complementaria para convertirse en el dominio preconditionante para el éxito de cualquier operación física moderna. Las Fuerzas de Defensa Globales asumen que el control del Espectro Electromagnético (EMS) y las autopistas informáticas digitales definen la viabilidad táctica en el terreno.

Las operaciones en el ciberespacio operan bajo una lógica asimétrica y de constante ambigüedad normativa. Conforme a las directrices de la Organización de las Naciones Unidas (ONU, 2020) sobre el impacto de las tecnologías digitales, las capacidades ciberoofensivas diluyen la atribución directa del ataque, lo que dificulta la aplicación de los principios clásicos de disuasión y el derecho de legítima defensa establecido en la Carta de las Naciones Unidas. Los ataques sofisticados dirigidos a los sistemas de control y adquisición de datos (SCADA) de las redes de energía o telecomunicaciones del oponente permiten alcanzar objetivos estratégicos de desestabilización nacional sin recurrir al despliegue físico de tropas blindadas o ataques de aviación estratégica.

Tecnología Emergente	Aplicación Operacional Primaria	Impacto Doctrina Militar	Desafío Crítico Identificado
Inteligencia Artificial Analítica	Automatización del Ciclo de Inteligencia (Targeting) y Mantenimiento Predictivo.	Reducción drástica del bucle de decisión OODA; Hyperwar.	Pérdida de control cognitivo humano; vulnerabilidad a sesgos algorítmicos.
Enjambres Autónomos (LAWS)	Saturación de sistemas defensivos enemigos; reconocimiento táctico avanzado.	Transición de plataformas tripuladas masivas a sistemas autónomos de bajo costo.	Ausencia de marcos éticos claros; riesgos de proliferación a actores no estatales.

Tecnología Emergente	Aplicación Operacional Primaria	Impacto Doctrina Militar	Desafío Crítico Identificado
Ciberoperaciones Ofensivas	Degradación de infraestructuras críticas y interrupción de sistemas C4ISR.	Guerra asimétrica de baja atribución; erosión de la distinción entre paz y guerra.	Dificultad extrema en la atribución; desestabilización social sistémica.
Computación Cuántica	Criptanálisis masivo y optimización logística en tiempo real.	Obsolescencia de los sistemas tradicionales de cifrado militar y diplomático.	Costo de desarrollo prohibitivo; carrera armamentista tecnológica asimétrica.

Tabla 6. Comparativa de Vectores Tecnológicos en Escenarios de Operaciones

Fuente: Elaboración propia en base a Comisión Económica para América Latina y el Caribe [CEPAL] (2021); Organización de las Naciones Unidas [ONU] (2020); y Centro de Estudios de las Fuerzas Armadas [CEFADIGITAL] (2021).

La Guerra Cognitiva y de la Información: El Cerebro Humano como Escenario Operativo

Las innovaciones tecnológicas de la última década han expandido las operaciones psicológicas y de propaganda hacia un concepto mucho más agresivo y sistemático: la Guerra Cognitiva. En este marco doctrinario, el objetivo final de las operaciones ya no radica en la destrucción material de las divisiones del oponente o en la captura física de sus capitales geográficas, sino en la alteración deliberada de las capacidades cognitivas, perceptivas y de toma de decisiones de la población civil y de los altos mandos estratégicos.

El desarrollo exponencial de la IA generativa facilita la creación y distribución masiva de contenidos sintéticos desinformativos de alta fidelidad, conocidos como Deepfakes. Estas herramientas tecnológicas permiten simular órdenes de comandantes en jefe, fabricar crisis diplomáticas artificiales o difundir ejecuciones falsas en plataformas digitales en tiempo récord, logrando desestabilizar la cohesión social de un país objetivo antes de iniciar operaciones de carácter cinético. Las redes sociales, alimentadas por sofisticados algoritmos de recomendación diseñados para maximizar la polarización emocional de los usuarios, funcionan como los vectores de entrega de estas armas informacionales, transformando el acceso a la información digital en una vulnerabilidad crítica para las sociedades de régimen democrático abierto.

Logística Avanzada, Sostenibilidad y la Resiliencia Industrial en el Frente del Futuro

El sostenimiento de un ejército desplegado en un escenario de operaciones moderno exige una transformación radical de las cadenas de suministro industriales y logísticas tradicionales. La integración de tecnologías asociadas a la denominada "Industria 4.0" en las estructuras de defensa busca mitigar una de las mayores debilidades históricas de las fuerzas expedicionarias: la dependencia de líneas de abastecimiento extensas y expuestas a la interrupción del enemigo.

La fabricación aditiva (Impresión 3D de alta precisión industrial) permite a las unidades militares desplegadas en entornos hostiles lejanos producir sus propias piezas de repuesto críticas al instante a partir de planos digitales codificados de forma segura en la nube logística. Esto reduce significativamente la necesidad de mantener grandes inventarios físicos de almacenamiento en el frente.

Por otra parte, la sostenibilidad energética emerge como un factor táctico y estratégico determinante en los teatros de operaciones futuros. Las fuerzas militares tecnificadas poseen un consumo energético sustancialmente mayor al del pasado debido a la necesidad constante de alimentar sistemas informáticos, procesadores de datos portátiles, baterías para drones y exoesqueletos de asistencia para los combatientes. El desarrollo e implementación de microredes de energía renovable portátiles y sistemas de almacenamiento energético de alta densidad disminuye la dependencia de los convoyes tradicionales de combustible fósil, los cuales representan históricamente uno de los objetivos más vulnerables para las tácticas de emboscada y ataques de guerra asimétrica del adversario.

Implicancias Éticas, Jurídicas y Geopolíticas de la Digitalización Militar

La transferencia progresiva de capacidades de decisión táctica y estratégica a sistemas gobernados por líneas de código informático e inteligencia artificial plantea cuestionamientos de índole moral y jurídica que el ordenamiento de los tratados internacionales vigentes no es capaz de resolver de manera efectiva.

El Derecho Internacional Humanitario frente a la Autonomía Militar

El pilar fundamental del Derecho Internacional Humanitario (DIH), codificado de forma principal en los Convenios de Ginebra, descansa sobre los principios de distinción, proporcionalidad y necesidad militar. Estos conceptos requieren la aplicación constante de juicios de valor humanos, empatía y evaluación del contexto cultural del conflicto en el terreno.

La programación actual de algoritmos de inteligencia artificial carece de la flexibilidad necesaria para distinguir de manera infalible a un combatiente legítimo de un civil herido o en actitud de rendición en un entorno urbano complejo y caótico. La ausencia de una conciencia humana en los sistemas de armamento automatizados plantea un vacío legal crítico respecto a la asignación de responsabilidades penales internacionales ante la comisión de crímenes de guerra originados por fallos o malas interpretaciones del código de software.

La Asimetría Norte-Sur y la Brecha Tecnológica Regional

La carrera armamentista por el dominio de las nuevas tecnologías acentúa las desigualdades estructurales del sistema internacional de estados. Los elevados requerimientos de capital financiero, infraestructura de supercomputación y talento científico calificado concentran el desarrollo de las capacidades militares disruptivas en un grupo sumamente reducido de potencias tecnológicas y empresas transnacionales oligopólicas.

Para las regiones en vías de desarrollo, como América Latina y el Caribe, este escenario plantea un doble desafío de vulnerabilidad estratégica. De acuerdo con los diagnósticos de transformación estructural elaborados por la CEPAL (2021), la persistencia de las brechas de conectividad digital básica e infraestructura industrial avanzada no solo obstaculiza el desarrollo económico nacional, sino que reduce la resiliencia sistémica de las instituciones de seguridad interna frente a amenazas transnacionales híbridas altamente tecnificadas, ensanchando la asimetría operativa frente a las potencias globales del norte global.

Conclusión

Hoy la seguridad y la soberanía de Paraguay van mucho más allá de cuidar las fronteras físicas que conocemos, ya que el verdadero desafío se trasladó al mundo digital, un escenario invisible pero que nos afecta a todos en el día a día. Las amenazas actuales, que van desde los ataques a servicios básicos hasta las noticias falsas que buscan dividirnos, nos obligan a repensar la forma en que nos protegemos como sociedad. Nuestro país está dando pasos importantes con la Política de Ciberdefensa Militar y el uso de tecnología en las fronteras, pero los drones y los sensores no pueden solucionar todo por sí solos. Al final del día, las computadoras y las herramientas digitales no sirven de nada sin el talento, el compromiso y la preparación de nuestra gente. El futuro de la defensa paraguaya depende enteramente de que apoyemos y capacitemos a profesionales que se animen a dejar atrás lo analógico para cuidar con éxito nuestro espacio digital.

Referencias

- Aionesei, G., & Panait, C. (2024). Understanding multi-domain operations from the air force perspective. *Review of the Air Force Academy*. <https://doi.org/10.19062/1842-9238.2024.22.1.8>
- Alvarado, J. M. (2022). La doctrina de las operaciones multi-dominio y el futuro de las fuerzas armadas en el siglo XXI. *Revista del Centro de Estudios de las Fuerzas Armadas (CEFADIGITAL)*, 18 (2), pp. 45-67.
- Babayev, S., Akhundov, R., & Hashimov, E. (2026). Conceptual-theoretical foundations and the transformative role of artificial intelligence in multidomain operations. *Grail of Science*. <https://doi.org/10.36074/grail-of-science.20.03.2026.069>
- Bustamante, R. (2023). Inteligencia artificial y el dilema de la velocidad de decisión en la guerra moderna. *Dialnet: Revista de Estudios Estratégicos*, 45 (1), pp. 112-134.
- Centro de Estudios de las Fuerzas Armadas. (2021). *Tecnologías disruptivas y escenarios operativos de defensa: Perspectivas doctrinales hacia 2035* (Monografía de Investigación N° 12). CEFADIGITAL.

- Centro de Estudios de las Fuerzas Armadas. (2024). *La ciberdefensa y la protección de infraestructuras críticas en la doctrina militar regional* (Documento de Trabajo N° 89). CEFADIGITAL.
- Clausewitz, C. von. (1984). *On war* (M. Howard & P. Paret, Eds. y Trans.). Princeton University Press. (Obra original publicada en 1832).
- Comisión Económica para América Latina y el Caribe. (2021). *Datos, algoritmos y políticas públicas: Hacia un desarrollo digital inclusivo y sostenible en América Latina*. Naciones Unidas.
- Cosmo Consult. (2024). *Tendencias tecnológicas para la próxima década: Inteligencia artificial, digitalización avanzada y sostenibilidad industrial*. Cosmo Consult Insights.
- Cranor, L. F. (2008). *A framework for reasoning about the human in the loop* (Reporte Técnico). Carnegie Mellon University.
- Fleck, D. (2019). *The law of future warfare and autonomous weapon systems*. Oxford University Press.
- Freedman, L. (2017). *The future of war: A history*. PublicAffairs.
- García, M. A. (2023). Ciberoperaciones tácticas y la degradación del espectro electromagnético en conflictos híbridos contemporáneos. *Revista Científica de Conducción Militar*, 29 (3), pp. 201-225.
- Godet, M., & Durance, P. (2011). *La prospectiva estratégica para las empresas y los territorios*. Marcombo.
- International Committee of the Red Cross. (2019). *Autonomous weapon systems: Implications of increasing autonomy in the critical functions of weapons*. <https://www.icrc.org/>
- Johnson, J. (2019). *Artificial intelligence and the future of warfare: The USA, China, and strategic stability*. Manchester University Press.
- Keohane, R. O., y Nye, J. S. (2012). *Power and interdependence* (4ª ed.). Longman.
- Li, J., Liu, Y., & Gu, L. (2010). DDoS attack detection based on neural network. En *2010 2nd International Symposium on Aware Computing* (pp. 196-199). IEEE. doi.org
- NATO. (2021). *NATO's approach to emerging and disruptive technologies*. North Atlantic Treaty Organization. <https://www.nato.int/>
- Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.

- Organización de las Naciones Unidas. (2020). *El impacto de las tecnologías digitales en el desarrollo global, la seguridad humana y la cooperación internacional*. Departamento de Asuntos Económicos y Sociales de las Naciones Unidas.
- Pavić, A., Jelic, D., & Đokić, M. (2024). Artificial intelligence as an asset for the improvement of decision-making cycle in military operations. *Vojno delo*. <https://doi.org/10.5937/vojdelo2403045p>
- Pedersen, F., & Jacobsen, J. (2024). Narrow windows of opportunity: the limited utility of cyber operations in war. *Journal of Cybersecurity*, 10 (1). <https://doi.org/10.1093/cybsec/tyae014>
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Sassen, S. (2007). *A sociology of globalization*. W. W. Norton & Company.
- Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
- Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
- Stensrud, R., Nummedal, O., & Valaker, S. (2024). Exploring human autonomy teaming methods in challenging environments: the case of uncrewed system (UxS) solutions—challenges and opportunities with artificial intelligence. *Human-Intelligent Systems Integration*, 6, pp. 115-130. <https://doi.org/10.1007/s42454-024-00058-4>
- United Nations Institute for Disarmament Research. (2020). *The weaponization of increasing autonomy: Artificial intelligence*. UNIDIR. <https://unidir.org/>
- U.S. Department of Defense. (2020). *DoD ethical principles for artificial intelligence*. <https://www.defense.gov/>
- Wogalter, M. S. (2006). *Handbook of Warnings*. CRC Press. <https://doi.org/10.1201/9781482289688>



CAPÍTULO UNDÉCIMO

PERÚ, CENTRO DE ALTOS ESTUDIOS NACIONALES DE PERÚ (CAEN)

De lo físico a lo cognitivo: nuevas tecnologías y la redefinición del campo de operaciones

Juan Fernando Ormachea Montes

Resumen: El presente artículo analiza cómo el desarrollo acelerado de nuevas tecnologías está transformando la naturaleza del campo de operaciones y redefiniendo los principios tradicionales de la guerra. Se sostiene que la evolución tecnológica ha ampliado los dominios operacionales más allá de los espacios físicos tradicionales, incorporando el ciberespacio y el dominio espacial, y dando lugar a un entorno multidominio caracterizado por la interconexión y la simultaneidad. Asimismo, se destaca el impacto de tecnologías emergentes como la inteligencia artificial, los sistemas no tripulados, el Big Data y las capacidades espaciales, las cuales están modificando la forma en que se planifican y ejecutan las operaciones. El artículo enfatiza que el conflicto contemporáneo se desplaza progresivamente hacia el dominio cognitivo, donde la información, la percepción y la toma de decisiones adquieren un papel central. En este contexto, la superioridad ya no depende exclusivamente de la capacidad destructiva, sino de la integración tecnológica, la gestión de la información y la capacidad de anticipación estratégica.

Palabras clave: Operaciones multidominio, inteligencia artificial, guerra cognitiva, ciberespacio, tecnologías emergentes.

Acerca del autor: Gral. Brig. EP **Juan Fernando Ormachea Montes**, Phd(c) .Doctor en Desarrollo y Seguridad Estratégica, Maestro en Ingeniería Electrónica con mención en telemática y Maestro en Ciencias Militares, Licenciado en Ingeniería Electrónica, actualmente es Docente y Analista Investigador del Centro de Altos Estudios Nacionales de Perú.

Introducción

En las primeras décadas de este siglo XXI, el escenario internacional ha experimentado una transformación acelerada promovida por el desarrollo exponencial de nuevas tecnologías (*World Economic Forum, 2023*). Este hecho no solo ha redefinido las dinámicas económicas y sociales, sino que está alterando profundamente la naturaleza de la seguridad y la defensa. En particular, la irrupción de tecnologías como la IA, el ciberespacio, los sistemas autónomos y el análisis masivo de datos está modificando de manera sustancial la forma en que los diferentes países conciben, preparan y ejecutan sus operaciones.

En este contexto, los escenarios operacionales han dejado de estar restringidos a los tradicionales espacios físicos para expandirse hacia dominios intangibles, interconectados y altamente dinámicos. Más aún, el centro de gravedad del conflicto está experimentando un desplazamiento progresivo desde lo físico hacia lo cognitivo, donde la información, la percepción y la influencia sobre la voluntad de los actores se convierten en elementos decisivos.

La competencia estratégica actual ya no se limita al control de un área geográfica o a la superioridad de material bélico, sino que se extiende al dominio de la información (*NATO, 2020*), la manipulación de esta información y la capacidad de incidir en los procesos de toma de decisiones tanto de adversarios como de poblaciones. En este nuevo entorno, el campo de operaciones se redefine como un espacio multidimensional donde convergen lo físico, lo virtual y lo cognitivo.

Asimismo, el creciente acceso a las actuales tecnologías ha disminuido las barreras de participación para los actores no estatales, quienes ahora pueden ser partícipes y generar efectos estratégicos significativos sin necesidad de contar con grandes capacidades militares convencionales. Este fenómeno ha incrementado la complejidad de los escenarios operacionales y reducido las fronteras entre paz y conflicto, generando escenarios de competencia continua en la

denominada “zona gris” donde se compite sin llegar a la guerra abierta, utilizando medios indirectos, encubiertos o no convencionales.

En este marco, el presente artículo sostiene que las nuevas tecnologías no solo están modernizando los escenarios operacionales, sino que están impulsando una transición estructural desde un enfoque centrado en lo físico hacia uno orientado al dominio cognitivo, redefiniendo así la naturaleza del campo de operaciones y los fundamentos de la seguridad y la defensa contemporánea.

Evolución del campo de operaciones: De lo físico al multidominio y cognitivo

La transformación de los tradicionales principios de la guerra:

Los principios de la guerra se han ligado siempre a la tecnología que había en cada época. En los conflictos de la antigüedad, el inicio de las operaciones se hacía con acciones de desgaste o de “ablandamiento”. Estas acciones buscaban debilitar al adversario antes del enfrentamiento directo. Estas acciones se materializaban inicialmente mediante el empleo de arcos y flechas, evolucionando posteriormente hacia el uso intensivo de la artillería, y más adelante, con la irrupción de la aviación militar, hacia campañas aéreas orientadas a neutralizar capacidades estratégicas y alcanzar la supremacía aérea.

En todos estos casos, el “desgaste inicial” o “ablandamiento” implicaba necesariamente un despliegue masivo de medios físicos, así como la concentración de fuerzas en el espacio y en el tiempo. La proximidad al adversario, el control del terreno y la superioridad material constituían factores determinantes para el éxito de las operaciones.

Sin embargo, en los escenarios actuales, este principio ha experimentado una transformación sustancial. El desarrollo de capacidades cibernéticas ha introducido una nueva modalidad de degradación (acciones previas al enfrentamiento), caracterizada por su naturaleza no física, su alcance global y alta precisión. En lugar de recurrir exclusivamente al empleo de armas que generan efectos mediante el impacto, explosiones o energía física, los actores pueden iniciar operaciones mediante ataques cibernéticos dirigidos contra sistemas de

armas, redes de comando y control, infraestructura crítica y sistemas de información.

Este tipo de acciones presenta varias características disruptivas. En primer lugar, no se requiere una aproximación física al adversario, lo que reduce significativamente los riesgos operacionales y las barreras geográficas. En segundo lugar, permite generar efectos estratégicos relevantes con una cantidad mínima de personal altamente especializado, en contraste con las grandes concentraciones de fuerzas que caracterizaban los conflictos tradicionales. Finalmente, estas operaciones pueden ejecutarse de manera encubierta, dificultando la atribución y ampliando el margen de acción en la denominada “zona gris”.

Por lo tanto, es hoy en día difícil definir cuando empiezan realmente las operaciones. A diferencia de los conflictos convencionales, donde existía una clara transición entre paz y guerra, en el entorno actual el accionar se caracteriza por una progresión latente que logra pasar desapercibida tanto para el enemigo como para la comunidad externa.

Este cambio no solo redefine los medios utilizados, sino que impacta directamente en los principios clásicos de la guerra, tales como la masa, la sorpresa, la concentración de fuerzas y la maniobra. En particular, la superioridad tecnológica y la capacidad de acceso para la explotación de la información prevalecen sobre la superioridad numérica o material.

Por eso el área de operaciones ya no se limita a lo que se toca. El área de operaciones ahora es un espacio donde lo digital y lo cognitivo dominan. Lo digital y lo cognitivo se vuelven parte del área de operaciones. Los sistemas pueden degradar capacidades sin destruir nada. Los sistemas pueden influir en la toma de decisiones del adversario. Los sistemas pueden cambiar la percepción de la realidad. El conflicto de hoy evidencia que el conflicto avanza hacia dimensiones que casi no se ven. Las dimensiones pueden decidir más y pueden actuar mejor..

La virtualización de las fases iniciales del combate: drones, ataques remotos y nuevas formas de contacto operacional

Los conflictos contemporáneos están evidenciando una transformación significativa en la forma en que se inician las operaciones. A partir de las lecciones observadas en escenarios recientes, como el conflicto entre Rusia y Ucrania, así como en las tensiones entre Estados Unidos e Irán, se aprecia una tendencia creciente hacia la reducción (e incluso eliminación) del enfrentamiento físico directo en las etapas iniciales del combate.

En contraste con los modelos tradicionales, donde el contacto cercano entre fuerzas constituía un elemento central para el inicio de las operaciones, en la actualidad se observa un predominio de acciones ejecutadas remotamente y a distancia mediante el empleo de vehículos aéreos no tripulados (UAV), sistemas autónomos y misiles de precisión. Estas capacidades permiten identificar, vigilar y neutralizar objetivos sin necesidad de exponer directamente a las fuerzas propias.

Este fenómeno puede ser entendido como un proceso de desmaterializar el combate en sus fases iniciales, en el cual los efectos se generan sin una presencia física inmediata en el área de operaciones. En este contexto, el "contacto" con el adversario ya no implica necesariamente proximidad geográfica, sino la capacidad de acceder a sus sistemas, detectar sus vulnerabilidades y actuar sobre ellas desde distancias seguras.

Asimismo, el empleo intensivo de drones y sistemas no tripulados ha modificado la lógica de ocupación del terreno. Antes de cualquier intento de control físico de un espacio en disputa, se ejecutan operaciones sistemáticas orientadas a degradar las capacidades del adversario mediante ataques de precisión, vigilancia persistente y saturación de objetivos. Este proceso no solo reduce los riesgos para las fuerzas propias, sino que también condiciona el entorno operacional, facilitando posteriores acciones terrestres.

Cabe destacar que estas capacidades no requieren necesariamente estructuras militares tradicionales de gran escala. Por el contrario, pequeños grupos altamente especializados, apoyados en tecnología avanzada, pueden generar efectos desproporcionados en relación con su tamaño, lo que redefine la relación entre masa, maniobra y poder de combate.

Por tanto, se observa que el campo de operaciones evoluciona hacia un espacio donde la distancia física pierde relevancia frente a la capacidad tecnológica, y donde el dominio del espectro electromagnético, la información y los sistemas autónomos se convierte en un factor decisivo. Esta tendencia refuerza la transición hacia escenarios en los que lo remoto y lo cognitivo adquieren primacía sobre el contacto físico directo.

Resulta además evidente que la naturaleza del campo de operaciones está experimentando una transformación profunda, en la cual la tecnología deja de ser un elemento de apoyo para convertirse en un factor central y decisivo en la conducción de las operaciones. La capacidad de anticipar, degradar y condicionar al adversario mediante medios tecnológicos redefine las fases del conflicto y altera los tiempos y espacios tradicionales de la confrontación. Así, el dominio tecnológico no solo amplía las capacidades operacionales, sino que también redefine los criterios de superioridad estratégica.

En consecuencia, en los escenarios actuales, la lucha o combate por el espacio se decide previamente en el dominio de la tecnología. Antes de la ocupación física del terreno, se libra una lucha silenciosa pero determinante en escenarios como el ciberespacio, el espectro electromagnético y los sistemas autónomos. El que logre imponer su superioridad en estos dominios no solo condicionarará el desarrollo de las operaciones, sino que establecerá las bases para el éxito en el terreno, consolidando así una nueva lógica en la conducción de la guerra, donde la tecnología se erige como el eje articulador del poder militar.

Tecnologías emergentes y su impacto en el campo de operaciones

El desarrollo disruptivo de nuevas tecnologías está configurando una nueva arquitectura del poder militar, que se caracteriza por la convergencia entre las capacidades digitales, sistemas autónomos y el procesamiento avanzado de información. Estas tecnologías no actúan de manera aislada, sino que se integran en ecosistemas operacionales complejos que redefinen la forma en que se planifican, conducen y evalúan las operaciones.

Más allá de su función como herramientas operativas, su verdadero impacto radica en que están alterando los principios tradicionales de la guerra, modifi-

cando la relación entre tiempo, espacio, masa y decisión. En este sentido, su incorporación no solo implica una modernización de capacidades, sino una transformación estructural del campo de operaciones.

A continuación, se analizan las principales tecnologías y su influencia en los escenarios operacionales contemporáneos:

Inteligencia Artificial (IA): Decisiones inmediatas y la guerra algorítmica

La inteligencia artificial (IA) se ha consolidado como un elemento transformador y crítico dentro de los paradigmas actuales de seguridad y la defensa. Su gran capacidad para el procesamiento de grandes volúmenes de datos en tiempo real permite optimizar la toma de decisiones, mejorar la precisión de las operaciones y anticipar las actividades del adversario.

En el ámbito operacional, la IA facilita la automatización de funciones críticas, desde la identificación de objetivos hasta la gestión de sistemas de armas autónomas. Esto da lugar a lo que algunos analistas denominan “guerra algorítmica” (*RAND Corporation, 2020*), donde la velocidad del procesamiento de información y la capacidad de respuesta automatizada ayudan a superar las limitaciones humanas.

Como consecuencia, el principio del “tiempo” adquiere una nueva dimensión: la ventaja ya no reside únicamente en la rapidez de despliegue de las fuerzas, sino en la capacidad de decidir más rápido y mejor que el adversario.

Un ejemplo concreto de estas capacidades se evidencia en sistemas de defensa antimisiles como el Iron Dome de Israel, donde el procesamiento automatizado de datos permite detectar amenazas, calcular trayectorias y estimar puntos de impacto en cuestión de milisegundos. Sobre la base de estos cálculos, el sistema puede priorizar objetivos y activar mecanismos de interceptación de manera prácticamente inmediata. Este tipo de soluciones evidencia cómo la integración de algoritmos avanzados y sistemas automatizados permite acelerar el ciclo de decisión a niveles que superan las capacidades humanas, reduciendo significativamente los tiempos de reacción y aumentando la eficacia operativa en entornos de alta complejidad.

Sin embargo, es importante mencionar que, en algunos enfoques contemporáneos, erróneamente la inteligencia artificial es percibida como una amenaza, especialmente cuando se plantea su potencial uso sin el control humano directo. Si bien es cierto que el empleo inadecuado o no regulado de estas tecnologías puede generar riesgos, la IA no constituye una amenaza intrínseca, sino una herramienta cuyo efecto final depende de la forma en que ha sido diseñada, implementada y supervisada. En este sentido, el desafío no radica en limitar su desarrollo, sino en establecer marcos éticos, normativos y operacionales que garanticen su uso responsable, manteniendo siempre el control humano sobre las decisiones críticas.

La IA ha evolucionado recientemente hacia la Inteligencia Artificial Generativa, la cual ofrece importantes ventajas operacionales. Su capacidad para procesar, sintetizar y generar información en múltiples formatos permite apoyar de manera directa la toma de decisiones en entornos muy complejos y dinámicos. A través de la generación automatizada de informes, la simulación de escenarios y la propuesta de cursos de acción, estas tecnologías contribuyen a mejorar la conciencia situacional, reducir la incertidumbre y optimizar los procesos de planificación. Esta IA generativa puede emplearse en todos los dominios operacionales, facilitando el análisis de grandes volúmenes de datos provenientes de sensores, sistemas de vigilancia y fuentes abiertas. En el ámbito cognitivo, permite analizar narrativas, identificar patrones de desinformación y generar respuestas informacionales oportunas. En consecuencia, su adecuada integración no solo incrementa la eficiencia operativa, sino que fortalece la capacidad de anticipación y adaptación, elementos clave en los escenarios de operaciones contemporáneos.

Esta evolución de la IA, obliga a tener nuevas consideraciones en el ámbito de la seguridad y la defensa. Estas tecnologías, capaces de producir contenidos altamente realistas (texto, imágenes, audio o video) pueden ser utilizadas tanto para apoyar procesos de análisis como para influir o distorsionar la percepción de la realidad. En escenarios operacionales, el uso indebido de IA generativa podría afectar la calidad de la información disponible, generar confusión en los decisores y alterar los procesos de toma de decisiones. En consecuencia, junto con sus beneficios, surge la necesidad de desarrollar capacidades que permitan validar la información, mitigar riesgos de manipulación y fortalecer la resiliencia frente a posibles distorsiones del entorno informacional.

La Inteligencia Artificial no solo decide más rápido, sino contribuye al entrenamiento en la toma de decisiones en realidades simuladas para lo cual utiliza datos sintéticos, entendidos como información generada artificialmente que reproduce patrones y comportamientos del mundo real sin provenir directamente de fuentes reales. Estos datos, producidos mediante modelos avanzados de IA, permiten entrenar sistemas, simular escenarios y desarrollar capacidades analíticas sin comprometer información sensible o clasificada.

Su utilización resulta particularmente relevante en el ámbito de la defensa, donde el acceso a datos reales puede estar limitado por razones de seguridad. A través de datos sintéticos, es posible recrear escenarios operacionales complejos, evaluar cursos de acción y mejorar la capacidad predictiva de los sistemas de inteligencia. No obstante, su empleo también plantea desafíos, ya que la validez de los resultados dependerá de la calidad y fidelidad con la que estos datos representen la realidad. En consecuencia, su integración debe ir acompañada de mecanismos rigurosos de validación que garanticen su confiabilidad en los procesos de toma de decisiones.

El Ciberespacio: el nuevo dominio invisible del conflicto

El ciberespacio se ha consolidado como el dominio central en los escenarios (ENISA, 2023) de operaciones contemporáneos. A través de él, es posible ejecutar acciones ofensivas y defensivas que afectan directamente las capacidades militares, económicas y sociales de un Estado.

Los ataques cibernéticos permiten degradar sistemas de comando y control, interferir comunicaciones, afectar infraestructuras críticas y generar desinformación, todo ello sin necesidad del contacto físico. Esta capacidad introduce un cambio significativo en el principio de maniobra, que ahora puede ejecutarse en entornos virtuales con efectos reales en el campo de operaciones.

Asimismo, el ciberespacio ha ampliado el espectro de actores, permitiendo la participación de actores no estatales con capacidades disruptivas, lo que incrementa la complejidad y la incertidumbre del entorno estratégico.

La relevancia del ciberespacio como dominio operacional se ha evidenciado con particular claridad en el contexto del conflicto entre Rusia y Ucrania, donde

las operaciones cibernéticas han acompañado de manera sistemática las acciones militares convencionales. Desde las fases iniciales del conflicto, se han registrado ataques dirigidos contra infraestructuras críticas (CSIS, 2023), redes gubernamentales y sistemas de comunicaciones, incluyendo el uso de malware destructivo como WhisperGate, diseñado para inutilizar sistemas informáticos.

El objetivo de estos ciberataques han sido degradar la capacidad de respuesta del Estado, afectar la coordinación institucional y generar incertidumbre en la población, evidenciando la inclusión del ciberespacio en las operaciones militares. Este caso demuestra que las operaciones cibernéticas no solo pueden preceder al empleo de la fuerza, sino también acompañarlo de manera persistente, configurándose como un componente esencial en la conducción del conflicto contemporáneo.

De igual forma, los ataques cibernéticos dirigidos contra infraestructuras energéticas en Ucrania en años recientes han puesto de manifiesto la vulnerabilidad de los sistemas críticos frente a este tipo de amenazas. La interrupción del suministro eléctrico mediante intrusiones en sistemas industriales evidencia la capacidad de los ciberataques para generar efectos directos sobre la vida cotidiana de la población, trascendiendo el ámbito militar y afectando la estabilidad social y económica.

Sistemas no tripulados y enjambres: La redefinición de la masa y el riesgo

El empleo de drones y vehículos autónomos (sistemas no tripulados), está transformando la forma en que se concibe el poder de combate. Estos sistemas permiten ejecutar misiones de reconocimiento, vigilancia y ataque con menor riesgo para el personal y a costos relativamente reducidos.

Resulta particularmente significativo el desarrollo de enjambres de drones, que operan de manera coordinada mediante algoritmos, saturando las defensas del adversario y generando efectos de grandes proporciones. A consecuencia de ello, el principio de masa ya no se refiere únicamente a la concentración de tropas o medios pesados, sino a la capacidad de generar volumen de efectos mediante sistemas distribuidos y coordinados.

De esta manera, la superioridad puede lograrse no por acumulación física, sino por densidad tecnológica y capacidad de coordinación.

Un ejemplo representativo del impacto de estos sistemas se observa en conflictos recientes como la guerra entre Rusia y Ucrania, donde el empleo intensivo de drones (tanto de reconocimiento como de ataque) ha modificado la dinámica del campo de batalla. El uso de vehículos aéreos no tripulados de bajo costo, incluidos drones comerciales adaptados con fines militares, ha permitido realizar tareas de vigilancia persistente, corrección de fuego de artillería y ataques de precisión contra objetivos tácticos.

Asimismo, el empleo de drones en forma de enjambres o en operaciones coordinadas ha demostrado la capacidad de saturar defensas convencionales, generando efectos desproporcionados frente a sistemas más costosos y complejos. Este fenómeno evidencia que la superioridad operativa ya no depende exclusivamente de plataformas tradicionales, sino de la capacidad de integrar tecnologías accesibles con conceptos innovadores de empleo.

Big Data y analítica avanzada: la supremacía de la información

El acceso y procesamiento de grandes volúmenes de datos (Big Data) permite obtener una comprensión más precisa y en tiempo real del entorno operacional. La integración de múltiples fuentes de información —sensores, inteligencia, redes sociales, entre otros— facilita la construcción de una imagen operativa común altamente dinámica.

Esto fortalece el principio de conocimiento del adversario, permitiendo anticipar sus acciones y reducir la incertidumbre. Asimismo, potencia la capacidad de operar en el dominio cognitivo, al facilitar la identificación de vulnerabilidades en la percepción y comportamiento de actores clave.

En este sentido, la información ha dejado de ser un recurso de apoyo para convertirse en un elemento central del poder operativo. El empleo de la Big Data no solo incrementa la cantidad de información disponible, sino que transforma cualitativamente los procesos de inteligencia. La integración y correlación de datos provenientes de múltiples fuentes (sensores, sistemas de vigilancia, comunicaciones, redes sociales y fuentes abiertas) permite generar análisis más

precisos, reduciendo los márgenes de incertidumbre y mejorando la calidad de la inteligencia producida. De esta manera, los sistemas de inteligencia evolucionan desde modelos reactivos hacia enfoques predictivos, capaces de anticipar comportamientos y detectar patrones antes de que se materialicen en acciones concretas.

La capacidad de procesar grandes volúmenes de información en tiempo casi real permite que la inteligencia resultante no solo sea más precisa, sino también más oportuna y relevante para la toma de decisiones. En los conflictos contemporáneos, como el desarrollado entre Rusia y Ucrania, el empleo combinado de imágenes satelitales, inteligencia de fuentes abiertas (OSINT) y análisis de datos ha permitido identificar movimientos de tropas, localizar objetivos y evaluar daños con una rapidez sin precedentes. Este tipo de capacidades nuevamente evidencia que la superioridad en el campo de operaciones ya no depende únicamente de la posesión de medios, sino de la capacidad de transformar datos en inteligencia accionable de manera eficiente y oportuna.

En este sentido, la ventaja estratégica se desplaza hacia aquellos actores capaces de dominar el ciclo de datos, transformando información masiva en conocimiento útil para la acción.

Tecnologías espaciales: la dependencia estratégica del dominio orbital

El dominio espacial se ha convertido en otro componente crítico de las operaciones modernas. Los sistemas satelitales proporcionan capacidades esenciales como comunicaciones, posicionamiento, navegación y vigilancia, que sustentan el funcionamiento de las fuerzas militares.

La creciente dependencia de estas tecnologías convierte al espacio en un ámbito de competencia estratégica, donde la capacidad de proteger, degradar o neutralizar activos espaciales puede tener un impacto decisivo en el desarrollo de las operaciones.

En consecuencia, el control del espacio ya no es solo una cuestión tecnológica, sino un factor determinante para garantizar la continuidad y eficacia de las operaciones en todos los demás dominios.

Asimismo, el dominio espacial no solo constituye un soporte crítico para las operaciones en otros ámbitos, sino que comienza a perfilarse como un posible escenario de confrontación directa. La creciente militarización del espacio, evidenciada en el desarrollo de capacidades antisatélite (ASAT), sistemas de vigilancia orbital y plataformas con potencial uso militar, ha dado lugar a la posibilidad de lo que comúnmente se ha denominado como una “guerra en el espacio”, en la cual los activos orbitales se convierten en objetivos estratégicos.

No obstante, a diferencia de los dominios tradicionales, el acceso y control del espacio se encuentra limitado a un número reducido de Estados que poseen capacidades tecnológicas avanzadas, lo que genera una marcada asimetría en este ámbito. Esta situación plantea desafíos significativos para la mayoría de países, que dependen de infraestructuras espaciales (propias o de terceros) sin contar necesariamente con los medios para protegerlas o sustituirlas.

En cuanto a la soberanía, el espacio ultraterrestre presenta particularidades jurídicas y estratégicas. De acuerdo con el marco normativo internacional, especialmente el Tratado del Espacio Ultraterrestre (*United Nations, 1967*), el espacio no puede ser objeto de apropiación nacional por ningún medio, lo que implica que ningún Estado ejerce soberanía en sentido tradicional sobre este dominio. Sin embargo, los Estados sí mantienen jurisdicción y control sobre los objetos espaciales que registran, como satélites y estaciones, lo que configura una forma de presencia e influencia indirecta en el entorno espacial.

En este contexto, el dominio espacial se consolida como un ámbito estratégico donde convergen intereses civiles, comerciales y militares, y cuya relevancia continuará en aumento. La capacidad de acceder, operar y proteger activos en este dominio será un factor determinante en la competencia estratégica futura, especialmente en escenarios donde la dependencia tecnológica y la vulnerabilidad de los sistemas orbitales pueden condicionar el desarrollo de las operaciones en los demás dominios.

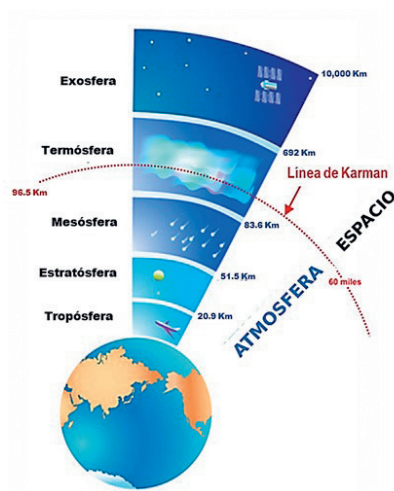


Figura 1. Zona de operaciones en el dominio espacial (a partir de la línea de Karman).

En este sentido, la superioridad en el dominio espacial no solo amplifica las capacidades en otros ámbitos, sino que puede condicionar decisivamente el resultado de las operaciones multidominio

A partir de la línea de Karman (~100 km de altitud), se establece convencionalmente el inicio del dominio espacial, donde se desarrollan operaciones relacionadas con sistemas satelitales, vigilancia, comunicaciones y capacidades estratégicas, constituyendo un nuevo escenario del campo de operaciones multidominio (U.S. Army, 2018).

La expansión de los dominios operacionales y la centralidad de los sistemas C4ISR

La incorporación de tecnologías y la ampliación de los dominios donde se desarrolla el conflicto han marcado la evolución del campo de operaciones. Durante mucho del siglo XX, se dirigía las operaciones en tres dominios, el dominio terrestre, el dominio del mar y el dominio del aire que formaron la base de la conducción. Cada dominio tenía las capacidades del dominio, las doctrinas del dominio y las formas del dominio para usar el poder de la fuerza.

El avance de la tecnología y la interdependencia de los sistemas han creado otros dominios que cambian la forma del conflicto. Primero, el dominio espacial

surgió como una un área de operaciones adicional. En el dominio espacial se consolidan las tele comunicaciones, el geo posicionamiento en todo el planeta, la navegación y la vigilancia. La dependencia de los sistemas de satélites hizo que este dominio del espacio sea necesario para las operaciones de hoy.

Después, con el desarrollo de la tecnología de la información y las comunicaciones hizo que el ciberespacio se convirtiera en un dominio de operaciones. El ciberespacio no es un elemento que se pueda tocar, el ciberespacio esta presente en todo el planeta y el ciberespacio se mueve con rapidez. Eso permite que el ciberespacio ejecute operaciones que ocurren en simultaneidad y que esas operaciones continúen sin límites de geografía.

La incorporación de estos dominios ha llevado la evolución a un enfoque de operaciones multidominio (U.S. Army, 2018). En ese enfoque, la efectividad depende de la capacidad de integrar y sincronizar las acciones en los dominios. En el contexto, la superioridad no se logra solo en un dominio. La superioridad se logra cuando la capacidad genera efectos al mismo tiempo.

En este caso, los sistemas de Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento (C4ISR) son muy importantes. Los sistemas de C4ISR juntan la información de varios dominios. Con esa información, los sistemas de C4ISR crean una visión operativa común y hacen que la toma de decisiones sea más rápida y de mejor calidad.

Los sistemas se vuelven más sofisticados y hacen que el dominio del espectro electromagnético sea más importante. En el espectro electromagnético la guerra electrónica tiene un papel clave. Proteger las propias comunicaciones, interferir las del adversario y controlar el flujo de información son factores importantes para asegurar la superioridad operacional.

La guerra electrónica adquiere relevancia en los conflictos, cuando el control del espectro electromagnético es una necesidad. En la guerra entre Rusia y Ucrania, los militares usan intensamente la interferencia electrónica para dañar el GPS, las comunicaciones y los enlaces de datos. La interferencia electrónica reduce la efectividad de los drones, de los sistemas de armas y de las estructuras de comando y control.

Estas acciones muestran que la guerra electrónica no solo ayuda, también funciona como herramienta de ataque y de defensa que condiciona el desarrollo de

las operaciones. Controlar el espectro electromagnético permite proteger las capacidades y también limitar o neutralizar las capacidades del adversario. Así la guerra electrónica consolida la posición de la guerra electrónica en el entorno multidominio.

La expansión de los dominios operacionales y la conexión de los sistemas tecnológicos han creado un entorno donde la información, la conectividad y el control del espectro electromagnético son partes clave del poder militar. En este nuevo escenario, los sistemas C4ISR y la guerra electrónica no solo ayudan a las operaciones. Los sistemas C4ISR y la guerra electrónica también son esenciales para llevar a cabo el conflicto en todos los niveles y en todos los dominios operacionales.

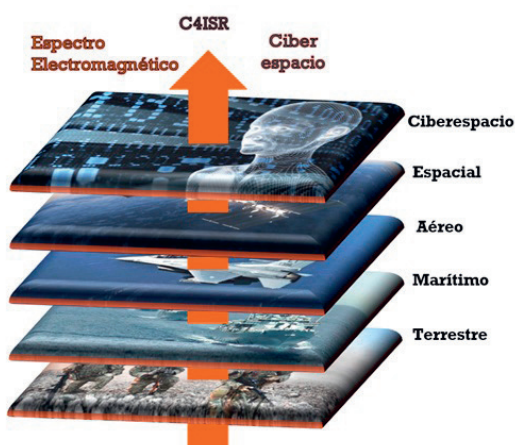


Figura 2. Arquitectura multidominio del campo de operaciones y transversalidad del espectro electromagnético, el ciberespacio y los sistemas C4ISR.

Los dominios terrestre, marítimo, aéreo, espacial y ciberespacial se integran en un entorno multidominio, donde los sistemas C4ISR y el control del espectro electromagnético actúan como elementos transversales que posibilitan la superioridad operativa.

En conjunto, estas tecnologías evidencian que el campo de operaciones contemporáneo está definido por la convergencia entre lo físico, lo digital y lo cognitivo, donde la superioridad ya no depende exclusivamente de la capacidad

destructiva, sino de la habilidad para integrar sistemas, procesar información y tomar decisiones en entornos complejos y altamente dinámicos.

En este nuevo paradigma, la tecnología no solo potencia las capacidades existentes, sino que redefine las reglas del conflicto, consolidando un entorno en el que la ventaja estratégica estará determinada por la capacidad de adaptación, innovación y dominio de estos nuevos recursos.

De la guerra física a la guerra cognitiva: La transformación del concepto de operaciones

La evolución de la tecnología y la expansión de las áreas de operación dieron lugar a un cambio. La evolución de la tecnología y la expansión de las áreas de operación están cambiando el concepto de operación. El conflicto ya no permanece en la pelea entre fuerzas. El conflicto ahora llega a la mente de las personas. Las personas forman percepciones, las personas moldean decisiones y las personas discuten la legitimidad.

Tradicionalmente, las operaciones militares destruyeron capacidades del adversario y controlaron el terreno. Hoy, las operaciones militares amplían el objetivo y buscan influir en la voluntad de los decisores políticos y de las poblaciones. El centro de gravedad del conflicto ya no está solo en el poder militar. El centro de gravedad del conflicto ahora está en la capacidad de afectar el pensamiento, la percepción y el comportamiento.

En este marco, emerge el concepto de guerra cognitiva (NATO, 2020), entendido como el conjunto de acciones destinadas a influir, alterar o controlar los procesos cognitivos del adversario. A diferencia de la guerra de la información (que se centra en el control y manipulación de contenidos), la guerra cognitiva tiene como objetivo final la mente humana, buscando incidir en la percepción, el juicio y la toma de decisiones.

Con las tecnologías digitales, con las plataformas de información, con la inteligencia artificial y con el análisis de datos, el equipo puede diseñar y ejecutar operaciones. Las operaciones pueden manipular narrativas, pueden generar desinformación y pueden explotar vulnerabilidades psicológicas y sociales.

A diferencia de las formas de confrontación que ya se usaban, la guerra cognitiva tiene rasgos que la separan de esas formas. El campo de acción de la guerra cognitiva no tiene límites; la guerra cognitiva no reconoce fronteras físicas ni temporales. Los efectos de la guerra cognitiva llegan al fondo y se mantienen en el tiempo; la guerra cognitiva afecta la cohesión social, la confianza en las instituciones y la estabilidad política. La guerra cognitiva se esconde; la guerra cognitiva dificulta que se identifique al agresor y que se dé una respuesta que sea la que corresponde, y la guerra cognitiva abre más espacio de maniobra en la competencia de estrategia.

Asimismo, el dominio de la cognición se conecta de cerca con otros ámbitos de operación, sobre todo el ciberespacio y el entorno de la información. Las operaciones en redes sociales, la manipulación de contenidos en línea y la explotación de algoritmos de difusión permiten ampliar mensajes y crear impactos con un alcance que se extiende mucho usando recursos que no alcanzan. Así la información se vuelve un vector de poder que puede producir efectos que se parecen y a veces superan a los que generan los medios de fuerza física.

El cambio de paradigma trae una definición del concepto de victoria. Los conflictos en el pasado medían el éxito por el control del territorio y por la destrucción del adversario. Los entornos de hoy buscan la victoria al alterar la percepción de la realidad, al deslegitimar al oponente y al inducir decisiones favorables sin necesidad de un enfrentamiento.

Por eso, las operaciones de hoy deben ser procesos que unen las acciones del físico, del digital y del cognitivo. La planificación y la conducción de las operaciones piden que se conozcan los factores culturales, los factores sociales y los factores psicológicos. También piden que se añadan las capacidades tecnológicas.

La transición de lo físico a lo cognitivo no elimina el combate usado antes. El combate usado antes queda bajo una lógica que incluye la fuerza y las acciones que moldean el entorno informacional y decisional del adversario. A veces las acciones aparecen antes de la fuerza.

Implicancias para la seguridad y defensa nacional

La transformación del campo de operaciones, impulsada por el avance de las tecnologías emergentes y el desplazamiento hacia el dominio cognitivo, plantea desafíos comunes para los sistemas de seguridad y defensa de los países del ámbito iberoamericano. En este contexto, las naciones enfrentan no solo la necesidad de adaptarse a nuevas formas de conflicto, sino también el reto de hacerlo en entornos caracterizados por limitaciones de recursos, dependencia tecnológica y dinámicas geopolíticas particulares.

En primer lugar, se evidencia la necesidad de actualizar los marcos doctrinarios, incorporando conceptos como las operaciones multidominio, la ciberdefensa, la guerra electrónica y la dimensión cognitiva del conflicto. Esta actualización resulta fundamental para garantizar que las fuerzas armadas puedan operar de manera efectiva en escenarios complejos, donde lo físico, lo digital y lo informacional convergen de manera simultánea.

En segundo lugar, el desarrollo de capacidades tecnológicas propias se presenta como un desafío estratégico para los países de la región. La dependencia de tecnologías externas puede generar vulnerabilidades críticas, especialmente en ámbitos sensibles como el ciberespacio, las comunicaciones y los sistemas de comando y control. En este sentido, se hace necesario promover políticas orientadas al fortalecimiento de la soberanía tecnológica y la cooperación regional en materia de innovación y desarrollo.

Asimismo, la formación del talento humano adquiere una relevancia central. Los nuevos escenarios operacionales demandan profesionales con competencias multidisciplinarias, capaces de integrar conocimientos técnicos, estratégicos y analíticos. Las instituciones académicas de defensa, particularmente aquellas que integran la comunidad iberoamericana, están llamadas a desempeñar un rol clave en la preparación de líderes capaces de enfrentar estos desafíos.

Otro aspecto fundamental es el fortalecimiento de la cooperación regional e interinstitucional. Dado que muchas de las amenazas contemporáneas (especialmente en el ciberespacio y el ámbito de la información) trascienden las fronteras nacionales, se requiere una mayor articulación entre Estados, así como entre los sectores público, privado y académico. En este contexto, espa-

cios como la Asociación de Colegios de Defensa Iberoamericanos (ACDIA) adquieren un valor estratégico como plataformas para el intercambio de conocimientos, experiencias y buenas prácticas.

De igual manera, la protección de la infraestructura crítica y de los sistemas de información se convierte en una prioridad compartida. La resiliencia de estos sistemas resulta esencial para garantizar la continuidad del funcionamiento del Estado y la estabilidad social frente a amenazas cada vez más sofisticadas.

En este entorno, el dominio del espectro electromagnético y del ciberespacio adquiere una dimensión estratégica transversal. La capacidad de proteger las propias redes, asegurar las comunicaciones y contrarrestar acciones adversarias en estos ámbitos será determinante para la eficacia de las operaciones y la preservación de la soberanía.

Finalmente, los países del ámbito iberoamericano deben fortalecer sus capacidades de anticipación estratégica, promoviendo el análisis prospectivo, la innovación y la adaptación continua. En un entorno caracterizado por la incertidumbre y la aceleración tecnológica, la capacidad de anticiparse a los cambios será un factor clave para garantizar la seguridad y la defensa en el largo plazo.

Los elementos analizados permiten establecer una visión integral sobre la transformación del campo de operaciones en el contexto contemporáneo.

Conclusiones y reflexiones

La evolución de la tecnología y la expansión de las áreas de operación provocan un cambio y cambian el concepto de operación. El conflicto ya no está solo en la pelea entre fuerzas. Ahora el conflicto llega a la mente de las personas. Las personas forman percepciones, las personas moldean decisiones y las personas discuten la legitimidad.

En el pasado, las operaciones militares destruían las capacidades del enemigo y controlaban el terreno. Hoy, las operaciones militares amplían el objetivo y tratan de influir en la voluntad de los políticos y de la población. El centro de gravedad del conflicto ya no está solo en el poder militar. El centro de gravedad

del conflicto ahora está en la capacidad de afectar el pensamiento, la percepción y el comportamiento.

En este marco, emerge el concepto de guerra cognitiva (NATO, 2020), entendido como el conjunto de acciones destinadas a influir, alterar o controlar los procesos cognitivos del adversario. A diferencia de la guerra de la información (que se centra en el control y manipulación de contenidos), la guerra cognitiva tiene como objetivo final la mente humana, buscando incidir en la percepción, el juicio y la toma de decisiones.

Con las tecnologías digitales, con las plataformas de información, con la inteligencia artificial y con el análisis de datos, el equipo puede diseñar y ejecutar las operaciones. Las operaciones pueden manipular la narrativa. Las operaciones pueden generar la desinformación. Las operaciones pueden explotar la vulnerabilidad psicológica y la vulnerabilidad social.

A diferencia de las formas de confrontación que ya se usaban, la guerra cognitiva tiene rasgos que la separan de las formas de confrontación. Su campo de acción no tiene límites. La guerra cognitiva no reconoce fronteras de espacio y de tiempo. Los efectos llegan al fondo y permanecen en el tiempo, afecta la cohesión de la sociedad, la confianza en las instituciones y la estabilidad del gobierno. Se esconde y complica la identificación del agresor. La guerra cognitiva complica la entrega de la respuesta correcta. La guerra cognitiva abre más espacio de maniobra en la competencia de estrategia.

El dominio del pensamiento se conecta con áreas, sobre todo con el ciberespacio y con el entorno de la información. Las actividades en redes sociales, el cambio de contenidos en línea y el uso de algoritmos de difusión hacen que los mensajes lleguen a más gente. Los mensajes causan impactos usando recursos. La información se convierte en una herramienta de poder y produce efectos que pueden igualar o superar los efectos de los medios de fuerza física.

El cambio de forma de ver las cosas trae un significado de la victoria. Antes los conflictos medían el éxito con el control del territorio y con la destrucción del enemigo. Hoy los entornos buscan la victoria cambiando la percepción de la realidad, deslegitimando al oponente y provocando decisiones que benefician y algunas veces sin necesidad de pelear.

Por eso, las operaciones de hoy deben unir la parte física, lo digital y el aspecto cognitivo. La planificación de las operaciones y la conducción de las operaciones requieren que se conozcan los factores culturales, los factores sociales y los factores psicológicos. También requieren que se añadan las capacidades tecnológicas.

La transición de lo físico a lo cognitivo no elimina el combate usado antes. El combate de enfrentamiento sigue bajo una lógica que incluye la fuerza y las acciones que moldean el entorno de información y de decisiones del adversario. A veces las acciones aparecen antes que la fuerza.

Referencias

- Center for Strategic and International Studies. (2023). *Significant cyber incidents database*.
- European Union Agency for Cybersecurity. (2023). *ENISA threat landscape report 2023*.
- North Atlantic Treaty Organization. (2020). *Cognitive warfare*. NATO Innovation Hub.
- RAND Corporation. (2020). *Artificial intelligence and national security*.
- U.S. Army. (2018). *The U.S. Army in multi-domain operations 2028 (TRADOC Pamphlet 525-3-1)*.
- U.S. Department of Defense. (2021). *Joint all-domain operations (JADO) strategy*.
- United Nations. (1967). *Treaty on principles governing the activities of states in the exploration and use of outer space*.
- World Economic Forum. (2023). *Global risks report 2023*.



CAPITULO DUODÉCIMO

PORTUGAL. INSTITUTO DA DEFESA NACIONAL (IDN):

Tecnologia, doutrina e ensino militar profissional no campo de batalha transparente. Tecnologia no campo de batalha moderno, adaptação doutrinária e ensino, formação e treino militares

Luís Fernando Machado Barroso
Pedro Nuno Antunes Ferreira

Resumo: Este ensaio analisa os desafios impostos pela tecnologia contemporânea no campo de batalha moderno, caracterizado por uma transparência crescente que fragiliza as doutrinas clássicas como a guerra de manobra. Partindo das lições aprendidas em conflitos recentes, como a guerra russo-ucraniana, os autores argumentam que a tecnologia, incluindo UAS, inteligência artificial e sensores persistentes, **não torna a doutrina irrelevante, mas exige uma revisão dos seus pressupostos. A transformação proposta abrange quatro dimensões fundamentais: adaptações doutrinárias baseadas na concentração distribuída de efeitos; adaptações operacionais em comando, logística e guerra eletrónica; mudanças na cultura organizacional** que favorecem a aprendizagem e a experimentação; e, crucialmente, elementos para a reforma do ensino militar profissional. O texto conclui que a vantagem militar futura dependerá menos da posse de sistemas tecnológicos e mais da capacidade institucional de formar oficiais dotados de julgamento adaptativo e pensamento estratégico, aptos a decidir em ambientes saturados de informação e doutrinariamente instáveis.

Palavras-chave: Transparência do Campo de Batalha; Tecnologia Militar; Doutrina de Manobra; Ensino Militar Profissional; Adaptação Institucional.

Sobre os autores: Major-General **Luís Fernando Machado Barroso**, PhD; os seus interesses de investigação incluem Estratégia, Operações Militares e Relações Cívico-Militares; publicações anteriores estão disponíveis em <https://orcid.org/0000-0001-7243-9109>; Área académica: Estudos Estratégicos e Relações Internacionais.

Tenente-Coronel **Pedro Nuno Antunes Ferreira**, PhD; os seus interesses de investigação incluem a evolução da guerra e os conflitos contemporâneos. As publicações anteriores estão disponíveis em <https://orcid.org/0000-0003-1038-6165>; Área académica: Estudos Estratégicos e Relações Internacionais.

Introdução

A tecnologia tornou-se uma das dimensões mais visíveis da transformação contemporânea da guerra. Unmanned Air Systems (UAS) de reconhecimento e ataque, sensores, satélites comerciais, inteligência artificial, comunicações digitais, sistemas de guerra eletrónica, *loitering munitions*, plataformas robóticas e redes de *targeting* têm alterado profundamente a forma como as forças militares observam, decidem, atacam, protegem e sustentam. No entanto, a transformação em curso não deve ser interpretada como uma simples substituição da guerra “antiga” por uma guerra “nova”, nem como a vitória automática da tecnologia sobre a doutrina. O que está em causa é algo mais sublime: a tecnologia está a mudar as condições de aplicação das forças militares, obrigando a uma revisão de pressupostos doutrinários, operacionais, culturais e estruturais.

O ponto de partida para este texto é a ideia de que o campo de batalha moderno se tornou tendencialmente mais transparente. A transparência não significa visibilidade absoluta, mas uma redução drástica da margem para movimentar, concentrar, emitir, abastecer ou comandar sem ser detetado. A ligação entre sensores, plataformas aéreas não tripuladas, análise algorítmica, fogos de precisão e disseminação rápida de informação faz com que unidades de manobra, postos de comando, centros logísticos, depósitos de munições e concentrações de blindados se transformem rapidamente em alvos. Consequentemente, as doutrinas que privilegiem a concentração física de forças, a proteção da retaguarda, a estabilidade dos postos de comando e a liberdade de manobra são colocadas em causa.

A guerra russo-ucraniana tem funcionado como laboratório empírico desta transformação, embora não deva ser universalizada de forma acrítica. Caron (2026) mostra que a proliferação de UAS contribuiu para a democratização do poder aéreo, para a vigilância persistente do campo de batalha e para a vulnerabilidade de equipamentos pesados; mas também alerta que ainda é prematuro concluir que os UAS produziram uma revolução definitiva da guerra. Taylor (2025), por sua vez, defende que o futuro das formações blindadas não é o seu abandono, mas a sua adaptação a uma manobra ofensiva integrada com UAS, sistemas robóticos, guerra eletrônica e defesa contra UAS. Buchholz (2025) aprofunda a lógica da sobrevivência ao propor que a dispersão deve ser entendida não apenas como separação física, mas como produção deliberada de incerteza no ciclo de *targeting* do adversário. Milevski (2024) acrescenta uma dimensão político-operacional essencial: em determinados teatros, como os Estados Bálticos, a defesa posicional e avançada pode ser mais adequada do que uma manobra operacional clássica, porque ceder território pode ser politicamente inaceitável e porque atravessar o campo de batalha intacto se tornou mais difícil.

Assim, o nosso argumento baseia-se na premissa de que a tecnologia não torna a doutrina irrelevante. Antes pelo contrário, torna a qualidade doutrinária, organizacional e educacional ainda mais importante. A vantagem militar passa a depender da capacidade de integrar tecnologia, doutrina, comando, logística, cultura organizacional e aprendizagem institucional. A força mais eficaz não será necessariamente aquela que possuir mais UAS, mais sensores ou mais algoritmos, mas aquela que conseguir transformar esses meios em práticas coerentes de emprego operacional, sustentação, proteção, decisão e adaptação. Esta transformação exige mudanças em quatro dimensões. Primeiro, adaptações doutrinárias: da concentração física para a concentração distribuída de efeitos; da dispersão espacial para a dispersão física, eletromagnética e cognitiva; da manobra como movimento para a manobra como criação de dilemas e janelas de oportunidade. Segundo, adaptações operacionais: comando e controlo resiliente, logística distribuída, guerra eletrônica orgânica, contra-UAS, e treino sob vigilância persistente. Terceiro, adaptações culturais e estruturais: maior tolerância à experimentação, aquisição rápida, integração de inovação civil, redução de rigidez hierárquica e valorização da iniciativa dos subordinados. Quarto, adaptação do ensino militar profissional, que deve for-

mar oficiais capazes de julgar, questionar, decidir e aprender em ambientes incertos, tecnologicamente densos e doutrinariamente instáveis.

A dimensão educativa, formativa e de treino é decisiva. Sookermany (2016) argumenta que a educação militar tradicional tende a privilegiar uniformidade, estrutura e *drills* pré-planeados, embora as operações militares exijam preparação para o desconhecido e o imprevisível. Henåker (2022), ao estudar estilos de decisão em *wargames*, mostra que o estilo dependente está associado à derrota, sugerindo que a capacidade de decidir autonomamente sob pressão não é apenas uma virtude abstrata, mas uma competência operacional. Marcel-la (2010) reforça que a estratégia deve ser ensinada como prática dinâmica, não apenas como conteúdo; isto exige casos, simulações, reflexão, pensamento crítico e integração entre teoria e experiência. Assim, o ensino militar profissional, a formação de oficiais e o treino militar realista não são complementos administrativos da transformação militar: são condições centrais para a converter em capacidade operacional.

Este texto organiza-se em doze partes. A primeira caracteriza o campo de batalha moderno e a relação entre transparência, letalidade e compressão do tempo de decisão. A segunda discute a tecnologia como fator de aceleração e de transformação doutrinária, evitando tanto o determinismo tecnológico como a rejeição conservadora. A terceira analisa as adaptações necessárias da guerra de manobra. Este ponto é determinante, uma vez que se considera a guerra de manobra como ponto central na doutrina militar contemporânea. A quarta aborda as adaptações operacionais em comando e controlo, logística, guerra eletrónica e sustentação. A quinta examina adaptações culturais e estruturais das forças militares. A sexta desenvolve o papel do ensino, da formação e do treino militares como motor da adaptação. A sétima propõe implicações curriculares para oficiais, especialmente aqueles que têm alguma experiência e maturidade. A oitava relaciona as funções de combate com a transformação institucional. A nona sintetiza uma proposta integrada de adaptação. A décima identifica riscos de adaptação incompleta e critérios de implementação. A décima primeira coloca o oficial no centro da transformação. A décima segunda propõe um modelo pedagógico de adaptação contínua, antes da conclusão final.

O campo de batalha transparente: visibilidade, letalidade e compressão temporal

O conceito de campo de batalha transparente descreve um ambiente em que movimentos, concentrações, emissões, padrões logísticos e estruturas de comando se tornam mais detetáveis por uma combinação de sensores técnicos e humanos. Esta transparência resulta da convergência de meios antes relativamente separados: UAS táticos, satélites comerciais, sensores terrestres, SIGINT, OSINT, câmaras térmicas, radares, comunicações digitais, redes sociais, algoritmos de fusão de dados e sistemas de apoio à decisão. A transformação não está apenas na quantidade de informação disponível, mas na redução do tempo necessário para transformar observação em aquisição e esta em fogo.

Caron (2026) sustenta que os UAS permitem uma compreensão direta e quase em tempo real da atividade inimiga, tornando muito mais difícil ocultar grandes concentrações de tropas ou equipamento. A sua metáfora dos UAS como “mil snipers no ar” é útil porque releva simultaneamente persistência, precisão e ubiquidade: o UAS não é apenas um sensor distante, mas um observador armado ou ligado a sistemas de fogos capazes de explorar vulnerabilidades antes difíceis de atingir. A vulnerabilidade dos carros de combate, viaturas blindadas, artilharia e meios logísticos aos UAS First-Person View (FPV) demonstra que a letalidade já não exige necessariamente plataformas caras ou superioridade aérea tradicional.

Contudo, a transparência não deve ser confundida com onisciência. Os sensores podem ser enganados, saturados, degradados ou privados de contexto. A guerra eletrónica pode interromper ligações, o terreno pode limitar observação, a meteorologia pode reduzir a eficácia de UAS, e a decepção continua a ser eficaz. A transparência é, portanto, uma tendência e não uma condição absoluta. Ainda assim, é suficiente para alterar o cálculo operacional: aquilo que antes podia ser concentrado por algum tempo com risco aceitável passa agora a exigir janelas temporais curtas, proteção ativa, camuflagem multispectral, controlo de emissões e preparação para deslocamento imediato.

A consequência mais direta é o problema da concentração física. A doutrina clássica valoriza a concentração de potencial de combate no ponto decisivo. Essa concentração continua necessária, mas o seu formato tem de mudar.

Grandes formações, depósitos centralizados, postos de comando extensos e colunas logísticas previsíveis elevam simultaneamente o valor do alvo e a confiança do adversário na sua identificação. Buchholz (2025) mostra que, em ambientes saturados de meios *Intelligence Surveillance and Reconnaissance* (ISR) apoiados por IA, os sistemas de *targeting* tendem a priorizar alvos de elevado valor, elevada certeza e baixo risco de aquisição. Assim, a sobrevivência já não depende apenas de escapar à deteção; depende de reduzir a confiança adversária no valor, função, continuidade e prioridade do alvo.

A compressão temporal é a segunda consequência. Wu (2026) argumenta que a Inteligência Artificial (IA) e os sistemas algorítmicos começam a alterar a arquitetura da decisão militar, particularmente em relação ao *targeting*, comando e coordenação. No caso ucraniano, sistemas de fusão de dados, *targeting* apoiado por IA e redes de UAS reduzem o tempo entre deteção e tiro. A clássica sequência observar-orientar-decidir-agir permanece relevante, mas é pressionada por ciclos de dados que operam a ritmos mais rápidos do que a deliberação humana tradicional. Isto cria aquilo que pode ser entendido como compressão cognitiva: o comandante deve decidir com menos tempo, mais informação, maior ambiguidade e consequências potencialmente imediatas.

A terceira consequência é o fim da retaguarda segura. A logística torna-se observável e atacável. Colunas logísticas, depósitos de combustível, oficinas, ambulâncias, pontos de transferência de munições, antenas de comunicações e geradores deixam de ser apenas apoio da manobra; tornam-se parte do campo de batalha. Caron (2026).

Vigilância e ataque por UAS, na qual praticamente tudo o que se move pode ser observado e adquirido. Esta realidade obriga a repensar a sustentação como função de combate exposta e não como processo administrativo situado fora da zona de combate.

Por fim, o campo de batalha transparente altera o sentido da proteção. A proteção já não é apenas blindagem, cobertura, dispersão ou defesa antiaérea. Inclui assinatura térmica, assinatura eletromagnética, perfil digital, padrões de deslocamento, comportamento logístico, disciplina de comunicações e capacidade de decepção. Proteger uma força significa gerir aquilo que ela revela sobre si própria. Em consequência, a sobrevivência passa a ser uma disputa sobre per-

ceção e confiança: o adversário não ataca apenas o que vê, mas aquilo que julga compreender suficientemente para justificar a alocação de fogos.

Tecnologia e doutrina: entre aceleração, adaptação e transformação

A interpretação da tecnologia na guerra contemporânea deve evitar dois erros. O primeiro é o determinismo tecnológico: a ideia de que UAS, IA ou robôs tornam obsoletas por si só as formas anteriores de guerra. O segundo é o conservadorismo doutrinário: a ideia de que a tecnologia é apenas mais uma ferramenta subordinada a princípios imutáveis e, portanto, não exige alterações profundas. A realidade situa-se entre estes extremos. A tecnologia acelera práticas existentes, modifica algumas e transforma outras quando permite distribuir a autoridade, altera estruturas de comando ou cria atividades no campo de batalha.

Wu (2026) trata esta tensão a partir da discussão sobre o *Modern System* de Stephen Biddle (2004), defendendo que a eficácia militar moderna depende menos da tecnologia per se do que da forma como as forças empregam doutrina, dispersam, procuram cobertura, ocultação, supressão, executam a manobra e integram armas combinadas. Esta perspetiva continua relevante porque impede que a tecnologia seja vista como substituto da competência militar. No entanto, Wu argumenta que a IA coloca novas questões porque não é apenas um meio material de destruição: é também uma tecnologia de processamento de informação, previsão e apoio ou mediação de decisão. Quando algoritmos recomendam alvos, comprimem ciclos de *targeting* ou coordenam plataformas autónomas, a tecnologia deixa de ser simples instrumento e começa a afetar a arquitetura da decisão.

A guerra russo-ucraniana revela um padrão misto. Em logística, ISR e compreensão situacional, a IA acelera práticas existentes ao melhorar velocidade, precisão e coordenação. Em *targeting* começa-se a alterar os procedimentos pelos quais decisões são autorizadas e executadas. Wu (2026) interpreta este processo como adaptação parcial, não ainda como substituição total da doutrina. Esta distinção é essencial para o nosso argumento: a tecnologia não torna a doutrina irrelevante, mas torna mais urgente a revisão das condições em que a doutrina opera.

Caron (2026) aplica raciocínio semelhante aos UAS. Estes têm efeitos notáveis, porque reduz risco para operadores, democratiza capacidades aéreas, aumenta a vigilância, permite ataques de baixo custo e ajuda atores mais fracos a reduzir assimetrias. Porém, Caron rejeita conclusões absolutas sobre a morte da manobra ou do carro de combate. A eficácia dos UAS depende da densidade do teatro, das contramedidas disponíveis, da guerra eletrónica, da doutrina adversária e da capacidade de integrá-los numa arquitetura operacional coerente. Utilizar UAS sem treino, logística, operadores, software, comunicações, manutenção e integração de fogos não produzem vantagem sustentada.

Taylor (2025) desenvolve esta linha ao defender que a próxima transformação da guerra terrestre será vencida por quem conseguir empregar UAS em manobra ofensiva. Para o autor, a solução não é abandonar as formações blindadas, mas adaptá-las a uma nova economia de letalidade em que matar se tornou mais barato do que proteger. O carro de combate e a infantaria mecanizada mantêm funções indispensáveis para penetrar defesas preparadas, apoiar a infantaria no combate próximo, conquistar e manter terreno, explorar oportunidades, mas só sobreviverão se integrados com UAS, *loitering munitions*, sistemas contra-UAS, guerra eletrónica e robôs.

A IA deve ser situada no seu contexto social, institucional e organizacional. O seu melhor uso não é necessariamente automatizar a guerra, mas reduzir a complexidade informacional para apoiar decisões humanas. Este ponto é decisivo para as forças militares: a vantagem tecnológica não decorre apenas da aquisição de sistemas, mas da capacidade de os integrar em práticas organizacionais, estruturas de comando, cultura de aprendizagem e formação de decisores. A tecnologia mal integrada pode aumentar problemas humanos, como enviesamento, excesso de confiança, burocratização, homogeneidade cognitiva, em vez de os resolver.

Assim, a tecnologia deve ser interpretada como fator de pressão sobre a doutrina. Ela acelera o tempo da guerra, aumenta a exposição, torna a concentração mais arriscada, fragiliza estruturas fixas, exige dispersão, amplia a importância da guerra eletrónica e torna a logística um alvo permanente. Mas a resposta não é puramente técnica. É doutrinária, operacional, cultural, estrutural e educativa.

Adaptações doutrinárias: reformular a guerra de manobra

A guerra de manobra mantém relevância porque a guerra continua a exigir iniciativa, surpresa, exploração de fraquezas, deslocalização do adversário e criação de dilemas. O que muda são os pressupostos que sustentavam a sua aplicação. A manobra clássica assumia, em muitos casos, a possibilidade de concentrar forças, ocultar movimentos, explorar brechas, atravessar o campo de batalha e sustentar o avanço com uma logística relativamente protegida. No campo de batalha transparente, estes pressupostos tornam-se problemáticos.

Milevski (2024) mostra que a manobra, embora dominante no pensamento militar ocidental, não deve ser tratada como dogma. No contexto báltico, a defesa de “cada centímetro” de território da NATO e a memória histórica da ocupação soviética tornam politicamente inaceitável a cedência deliberada de espaço para posterior contra-ataque. Além disso, a fronteira russa limita a possibilidade de manobra ofensiva profunda da NATO; mesmo uma contraofensiva bem-sucedida tenderia a terminar na fronteira, regressando a uma situação defensiva. O argumento é relevante para além dos Bálticos: a doutrina deve ser subordinada ao contexto político e geográfico. A manobra não é sempre a solução preferível:

- A primeira adaptação doutrinária consiste, portanto, em substituir a oposição simples entre manobra e defesa posicional por uma combinação de defesa avançada, profundidade, elasticidade tática e contra-ataques seletivos. A defesa moderna não deve ser rígida, mas também não pode depender sempre da cedência operacional de território. Deve integrar fortificações, obstáculos, UAS, fogos de precisão, minas, sensores, defesa contra-UAS, guerra eletrónica, unidades móveis para contra-ataque e planeamento de proteção civil. A linha defensiva não é um regresso à passividade; pode ser uma arquitetura ativa de desgaste, canalização, deteção e destruição.
- A segunda adaptação é a passagem da concentração de forças para a concentração de efeitos. A guerra continua a exigir massa, mas a massa física torna-se vulnerável. Por isso, a doutrina deve privilegiar forças dispersas capazes de sincronizar fogos, UAS, ciber, guerra eletrónica, reconhecimento, artilharia, logística e manobra no momento decisivo. A concentração passa a ser temporal, funcional e informacional, não necessariamente geo-

gráfica. O objetivo é gerar superioridade local sem oferecer ao adversário um alvo compensador.

- A terceira adaptação é entender a dispersão como incerteza. Buchholz (2025) argumenta que a dispersão não deve ser pensada apenas como separação física. Num ambiente em que sensores e algoritmos procuram padrões, funções e prioridades, a dispersão deve criar dúvida. No domínio físico, isto exige múltiplos postos de comando pequenos, nós logísticos redundantes, ausência de padrões previsíveis, separação de funções valiosas e deslocamentos irregulares. No domínio eletromagnético, exige gestão de emissões, janelas aleatórias de comunicação, alternância de meios, falsos positivos e utilização de assinaturas ambíguas. No domínio cognitivo, exige operações desenhadas para confundir a interpretação adversária sobre intenção, valor e continuidade. A força não desaparece; torna-se difícil de reconhecer.
- A quarta adaptação é a integração da decepção como competência normal de manobra. A decepção não pode ser uma função episódica ou reservada a escalões superiores. No campo de batalha transparente, todas as unidades produzem assinaturas; logo, todas podem contribuir para manipular percepções. *Decoys*, falsos postos de comando, emissões simuladas, padrões logísticos enganosos, movimentos não padronizados e narrativas operacionais contraditórias podem reduzir a confiança dos sistemas adversários de *targeting*. Quanto mais transparente se torna o campo de batalha, mais importante se torna a capacidade de fabricar opacidade.
- A quinta adaptação é a manobra humano-máquina. Taylor (2025) sugere que a manobra ofensiva futura exigirá UAS lançados a partir de plataformas móveis, sistemas contra-UAS em camadas, guerra eletrónica ágil, robôs de brecha descartáveis e forças tripuladas capazes de explorar e manter terreno. O assalto robótico ucraniano referido pelo autor, embora limitado pela necessidade de substituição rápida por tropas humanas, mostra que robôs podem criar oportunidades, mas não substituem ainda a presença humana no desenvolvimento da situação e na manutenção do terreno. A doutrina deve, portanto, conceber UAS e robôs como parte da equipa de armas combinadas, não como alternativa total à manobra terrestre.

- A sexta adaptação é a revisão da noção de surpresa. A surpresa operacional clássica torna-se mais difícil, mas não impossível. Ela passa a depender menos de esconder tudo e mais de saturar, enganar, degradar ou confundir o sistema adversário. Surpresa pode significar a criação de uma janela temporária de ocultação por guerra eletrônica, lançar UAS de direções inesperadas, usar padrões logísticos falsos, atacar através de um domínio não antecipado ou explorar a rigidez interpretativa de algoritmos e analistas. A surpresa moderna é muitas vezes uma surpresa de interpretação, não apenas de localização.

Estas adaptações não eliminam a guerra de manobra. Reformulam-na. A manobra deixa de ser sobretudo movimento de plataformas concentradas e passa a ser a capacidade de criar dilemas sob vigilância persistente, sincronizando efeitos distribuídos e preservando coerência operacional em condições de dispersão.

Adaptações operacionais: comando, logística, guerra eletrônica e sustentação

- As adaptações doutrinárias só têm valor se forem traduzidas em práticas operacionais. O primeiro domínio é o comando e controlo. No campo de batalha transparente, postos de comando grandes, fixos, com emissões intensas e padrões previsíveis tornam-se alvos prioritários. Buchholz (2025) defende arquiteturas de comando e controlo (C2) conscientes da dispersão: postos de comando pequenos, móveis, redundantes e de baixa assinatura; planos de comunicação PACE¹; capacidade de transferência de controlo; comando-missão em vez de microgestão. A finalidade não é restaurar o C2 tradicional em condições dispersas, mas reinventá-lo.
- Esta reinvenção implica aceitar que a coerência não depende de conectividade permanente. Em ambientes de guerra eletrônica, *Global Positioning*

¹ Em termos militares, o acrónimo PACE refere-se a uma metodologia de planeamento de comunicações em quatro níveis de redundância: Primário, Alternativo, Contingência e Emergência. Este sistema garante que a equipa tem métodos de recurso imediatos para manter a coesão e o sucesso da missão.

System (GPS) degradado e *targeting* a nós de comando, as unidades devem conseguir operar com base na intenção do escalão superior, prioridades claras e limites de decisão. O comandante deve definir efeitos pretendidos, critérios de risco, prioridades de fogos, regras de emissão, janelas de convergência e condições de recomposição. A unidade subordinada deve ter autoridade, treino e confiança para agir sem esperar por validação constante.

- Contudo, dispersão sem coerência transforma-se em fragmentação. Buchholz (2025) alerta que existe um ponto de equilíbrio entre a dispersão necessária para sobreviver e a agregação necessária para sincronizar. A formação e o treino devem explorar este ponto. Unidades excessivamente dispersas podem sobreviver, mas perdem capacidade de concentrar efeitos. Unidades excessivamente concentradas podem manter o controlo, mas tornar-se alvos. A arte operacional moderna reside em ajustar esse equilíbrio em relação ao terreno, ameaça, missão e disponibilidade de comunicações.
- O segundo domínio é a logística. A sustentação deve deixar de ser concentrada, previsível e dependente de grandes nós. A doutrina logística deve incorporar módulo reduzidos, pré-posicionamento disperso, rotas variáveis, reabastecimento noturno, baixa assinatura térmica e eletromagnética, manutenção avançada, redundância de fornecedores, uso de UAS ou veículos não tripulados para pequenas cargas e planeamento de evacuação sob vigilância. Se a logística é alvo, a logística deve manobrar. Isto significa que unidades logísticas precisam de capacidades de proteção, camuflagem, contramedidas contra UAS, comunicações resilientes e treino em ambiente contestado.
- A terceira área é a guerra eletrónica. Taylor (2025) afirma que formações blindadas futuras devem manobrar no espectro eletromagnético com a mesma agilidade com que manobram no terreno. Isto exige capacidade orgânica de deteção, *jamming*, mudança de *waveform*, proteção de comunicações e supressão temporária de redes adversárias. A guerra eletrónica deixa de ser apoio especializado e torna-se condição da manobra. Sem controlo ou manipulação mínima do espectro, UAS podem ser perdidos, comunicações localizadas e unidades expostas.

- Buchholz (2025) aprofunda esta ideia ao rejeitar o entendimento simplista de disciplina de emissões como silêncio absoluto. O silêncio pode ser tão revelador quanto a emissão, sobretudo em ambientes saturados de assinaturas civis e militares. A alternativa é a dispersão eletromagnética: perfis variáveis, comunicações em janelas irregulares, alternância entre rádio, satélite, meios civis e analógicos, e criação deliberada de falsos positivos. O objetivo é impedir que o adversário execute o ciclo *targeting* suficientemente confiante.
- A quarta área é a defesa contra UAS. O contra-UAS deve ser organizado em camadas: detecção visual, acústica, radar e eletromagnética; *jamming*; armas cinéticas de curto alcance; redes, gaiolas e proteção física; camuflagem térmica; treino de reação a FPV; e procedimentos de deslocamento rápido. A proteção contra UAS não é apenas tecnológica, mas comportamental. Unidades devem aprender a não se agrupar, a reduzir a exposição, a explorar a cobertura, a mover sob condições meteorológicas favoráveis, a ocultar padrões logísticos e a operar com escotilhas fechadas quando necessário.
- A quinta área é a engenharia de combate. A brecha tradicional concentra meios, tempo e pessoas sob observação e fogo. Taylor (2025) propõe robôs de brecha simples, baratos, reconfiguráveis e descartáveis. Esta proposta tem implicações doutrinárias profundas: abrir passagem em obstáculos densos deve tornar-se uma “operação multidomínio” que combina robôs terrestres, UAS de ISR, fogos de supressão, guerra eletrônica, fumos, decepção e exploração por forças tripuladas.
- A sexta área é o treino de sobrevivência sob vigilância. Todas as tarefas táticas devem ser reconsideradas à luz da ameaça persistente de UAS e sensores. Patrulhas, montagem de postos de comando, reabastecimento, evacuação médica, concentração de reservas, artilharia, deslocamentos administrativos e reuniões de comando devem ser treinados como atividades observáveis e atacáveis. O treino realista deve incluir UAS inimigos simulados, comunicações degradadas, GPS negado, ataques a logística, perda de C2, *targeting* a postos de comando e necessidade de recomposição.

Adaptações culturais e estruturais: da eficiência burocrática à aprendizagem adaptativa

A tecnologia cria exigências estruturais que as forças militares nem sempre conseguem absorver. Organizações militares modernas tendem a valorizar previsibilidade, controlo, hierarquia, padronização e eficiência. Estes valores são necessários para gerar disciplina e escala, mas podem tornar-se obstáculos quando a inovação ocorre em ciclos curtos, quando o adversário se adapta rapidamente e quando soluções locais emergem antes de processos formais de aquisição e doutrina.

A guerra russo-ucraniana evidencia a importância da aprendizagem rápida. Wu (2026) compara a inovação descentralizada ucraniana com padrões mais centralizados de adaptação russa. A Ucrânia explorou UAS de baixo custo, redes voluntárias, inovação civil, desenvolvimento rápido de *software*, *targeting* distribuído e experimentação operacional. A lição não é que todas as forças devam copiar o modelo ucraniano, mas que a velocidade de aprendizagem se tornou parte da eficácia militar. Quem aprende mais depressa reduz a distância entre falha e adaptação.

A defesa contemporânea depende cada vez mais de empresas tecnológicas, serviços de *cloud*, satélites privados, software comercial, IA, comunicações civis e *startups*. Esta dependência pode acelerar inovação, mas também cria vulnerabilidades: soberania tecnológica, influência privada sobre política de defesa, dependência de fornecedores, risco de homogeneidade de dados e dificuldade de controlo democrático. Estruturalmente, as forças militares devem aprender a cooperar com a indústria civil sem se tornarem reféns dela.

A cultura organizacional deve mudar em quatro linhas. Primeiro, maior tolerância ao erro controlado. A inovação em UAS, guerra eletrónica e software exigem experimentação; se todos os erros forem penalizados como falhas de disciplina, a organização deixará de aprender. Segundo, maior abertura à diversidade cognitiva. Sookermany (2016) defende a diferença e a pluralidade como instrumentos de preparação para o imprevisível; isto é relevante para equipas militares que precisam de combinar oficiais operacionais, engenheiros, analistas, operadores de UAS, especialistas de dados, logísticos e peritos em ciber. Terceiro, maior descentralização real. O comando-missão não pode ser

apenas retórica; exige confiança, educação e aceitação de iniciativa subordinada. Quarto, maior capacidade de desaprendizagem. Doutrinas válidas num contexto podem tornar-se perigosas noutro.

A estrutura das forças deve refletir estas mudanças. Unidades de manobra precisam de operadores de UAS, técnicos de GE, analistas de dados, equipas contra-UAS e elementos de manutenção rápida. Brigadas e batalhões precisam de células de experimentação e integração tecnológica. A logística deve ter meios orgânicos de proteção e dispersão. Os postos de comando devem ser menores e modulares. Os exercícios devem integrar inovação tecnológica como variável normal, não como demonstração ocasional.

A cultura de classificação entre “combatente” e “técnico” também deve ser revista. No campo de batalha moderno, o operador de UAS, o programador que adapta software, o especialista em frequências e o logístico que redesenha rotas sob ameaça participam diretamente na produção de efeitos. A distinção entre frente e retaguarda, combatente e apoio, físico e digital torna-se menos nítida. Isto exige carreiras, incentivos e modelos de autoridade que valorizem competências técnicas sem as separar da compreensão tática.

O ensino, a formação e o treino militares como motor da adaptação

A adaptação doutrinária, operacional, cultural e estrutural depende do ensino, da formação e do treino militares. Não porque as escolas militares possam prever todas as tecnologias futuras, mas porque podem formar oficiais capazes de aprender, julgar, adaptar e treinar as suas unidades para operar sob incerteza. O ensino militar profissional deve deixar de ser entendido apenas como transmissão de doutrina consolidada. Deve ser concebido como espaço de maturação profissional, onde experiência, teoria, história, tecnologia, treino prático e reflexão crítica se combinam.

Importa distinguir três dimensões complementares. O ensino militar profissional desenvolve compreensão conceitual, pensamento estratégico, capacidade crítica e enquadramento histórico-doutrinário. A formação militar molda identidade profissional, ethos, liderança, responsabilidade, disciplina intelectual e cultura de comando. O treino militar transforma conhecimento e intenção em

desempenho repetível sob pressão, através de exercícios, simulações, *wargaming*, treino de campo e análise pós-ação. O erro seria separar estas dimensões. No campo de batalha transparente, o oficial precisa de compreender, querer e conseguir agir: compreender o ambiente, assumir responsabilidade e executar com proficiência em condições degradadas.

Sookermany (2016) oferece uma crítica particularmente relevante. Para o autor, a educação militar tradicional é marcada por uma visão modernista, orientada para universalismo, estrutura, objetividade, uniformidade e treino de respostas pré-planeadas. Contudo, as operações militares são inevitavelmente marcadas pelo desconhecido e pelo imprevisto. Por isso, a educação deve preparar para o imprevisível. O seu contributo não é rejeitar disciplina ou treino, mas introduzir uma pedagogia capaz de cultivar julgamento profissional por meio de emancipação, desconstrução, vocabulário, diálogo, diversidade e estética.

A emancipação significa libertar-se de pressupostos naturalizados. Para oficiais com maturidade, este ponto é decisivo. A experiência acumulada é um recurso, mas também pode cristalizar certezas: a crença de que a blindagem garante proteção suficiente; que a logística opera na retaguarda; que o posto de comando deve concentrar staff; que o controlo é superior à autonomia; que a tecnologia é uma capacidade especializada e não um ambiente transversal. A formação de oficiais experientes deve trabalhar sobre estes pressupostos, não apenas acrescentar conteúdos novos.

A desconstrução implica questionar conceitos e doutrinas. Termos como manobra, massa, surpresa, defesa, retaguarda, comando, sustentação, superioridade aérea e proteção devem ser revisitados. O objetivo não é relativismo doutrinário, mas maturidade conceptual. Um oficial deve ser capaz de perguntar: em que condições este princípio continua válido? Quando se torna perigoso? Que pressupostos tecnológicos, logísticos e políticos o sustentam? Que alternativa existe? Esta capacidade é essencial num ambiente em que o significado operacional de conceitos clássicos muda rapidamente.

O vocabulário é igualmente importante. Sookermany (2016) defende que linguagem e pensamento influenciam a ação. Se a doutrina continua a usar categorias herdadas sem as redefinir, pode impedir a adaptação. Por exemplo, “dispersão” como simples espaçamento físico não capta a necessidade de incerteza

eletromagnética e cognitiva; “logística” como apoio não capta a sua exposição como alvo; “UAS” como equipamento não capta a sua função simultânea de sensor, arma, nó de informação e instrumento psicológico. O ensino deve desenvolver vocabulário para pensar a guerra emergente.

O diálogo, as narrativas e os casos são instrumentos de julgamento. A estratégia é processo dinâmico de interação entre atores, escolhas e ambiente, exigindo avaliação, reavaliação e ajustamento constantes. O ensino da estratégia, por isso, também deve ser dinâmico. Casos históricos, *wargames*, simulações e debates obrigam os oficiais a confrontar a distância entre teoria e realidade, entre intenção e consequência, entre plano e fricção.

Henåker (2022) acrescenta uma dimensão empírica relevante: estilos de decisão importam. No seu estudo com 104 oficiais e académicos, o estilo dependente aparece significativamente ligado à derrota em *wargame*. O resultado não prova que a dependência cause sempre derrota, mas sugere que contextos táticos dinâmicos penalizam decisores que necessitam excessivamente de validação externa. Num campo de batalha disperso, onde comunicações podem falhar e ciclos de *targeting* são curtos, a dependência decisória pode significar perda de iniciativa. O ensino militar deve, portanto, desenvolver autoconsciência decisional: como cada oficial decide, que enviesamentos possui, quando procura demasiada informação, quando evita risco, quando decide por impulso e quando a intuição é experiência condensada.

A intuição merece atenção particular. Henåker (2022) mostra que estilos intuitivos e espontâneos podem ter vantagens em situações rápidas, mas também riscos. A intuição profissional não deve ser romantizada como talento natural. Deve ser cultivada por estudo, experiência, repetição, reflexão e feedback. A arte da estratégia não pode ser ensinada como algoritmo, mas a educação pode criar as bases para a intuição estratégica por meio de história, casos, simulações, reflexão e exposição a problemas variados (Marcella, 2010).

O treino militar deve complementar esta maturação intelectual. Sookermany critica uma educação reduzida a *drills* pré-planeados, mas isso não significa que os drills deixem de importar. A diferença é que o treino deve deixar de preparar apenas respostas previstas e passar a criar proficiência em ambientes imprevisíveis. Unidades e oficiais devem repetir procedimentos técnicos, mas em cenários que introduzam UAS inimigos, perda de comunicações, *jam-*

ming, GPS negado, *targeting* sobre postos de comando, evacuação médica sob vigilância e ataques à logística. O treino deve gerar automatismos úteis sem bloquear a adaptação.

A formação de oficiais com maturidade deve, assim, ser diferente da formação inicial. Oficiais experientes não precisam apenas de adquirir informação; precisam de reaprender, comparar, reconstruir e transformar experiência em julgamento adaptativo. A sua formação deve incluir ambientes de decisão ambíguos, adversários adaptativos, tecnologia falível, dilemas éticos, comunicação degradada, logística atacada, pressão temporal e necessidade de assumir responsabilidade sem garantias. A maturidade profissional não é apenas anos de serviço; é capacidade de rever pressupostos à luz de novas condições.

Implicações curriculares para educação, formação e treino de oficiais

A transformação do campo de batalha exige um currículo de ensino militar profissional organizado em torno de problemas, não apenas disciplinas. As áreas clássicas — tática, operações, estratégia, logística, liderança, direito, ética, tecnologia, história militar — devem continuar presentes, mas integradas em cenários que obriguem os oficiais a tomar decisões complexas. Para oficiais com alguma maturidade, o objetivo não é apenas atualizar conhecimentos, mas reconfigurar a relação entre experiência, doutrina e inovação:

- Primeira implicação: o currículo deve incluir literacia tecnológica operacional. Nem todos os oficiais precisam de ser engenheiros, mas todos precisam de compreender como UAS, IA, sensores, guerra eletrónica, ciber, OSINT, comunicações digitais e sistemas autónomos afetam manobra, proteção, logística e comando. Literacia tecnológica significa saber perguntar: que assinatura produzimos? Que dados alimentam o sistema adversário? Que dependências temos? Que acontece se o GPS falhar? Que alternativa analógica existe? Que riscos éticos surgem no *targeting* assistido por IA?
- Segunda implicação: o ensino deve incluir *wargaming* sistemático. *Wargames* não replicam a guerra, mas permitem observar decisão, adaptação, iniciativa, passividade e estilos de comando. Henåker (2022) demonstra que *wargames* podem ser usados para estudar a relação entre estilos de decisão e resultados táticos. No ensino, devem expor oficiais a adversários

criativos, consequências não lineares e necessidade de revisão de planos. O *wargame* deve ser seguido de análise pós-ação centrada não apenas no resultado, mas no raciocínio: que pressupostos foram considerados? Que informação foi ignorada? Quando se perdeu iniciativa? Que sinais indicavam mudança?

- Terceira implicação: os estudos de caso devem ser diversificados. Os casos históricos ajudam a desenvolver pensamento estratégico porque expõem os alunos a problemas que não cabem em modelos mecânicos. No contexto atual, os casos devem incluir Ucrânia, Nagorno-Karabakh, Iraque, Bálticos, campanhas de contrainsurgência, falhas logísticas, operações de decepção, crises ciber e casos não militares de adaptação organizacional. Casos fora da zona de conforto militar são úteis porque obrigam oficiais a reconhecer padrões em contextos diferentes.
- Quarta implicação: a avaliação deve privilegiar a qualidade do julgamento. Avaliar apenas a conformidade com procedimentos incentiva respostas padronizadas. Avaliar julgamento implica observar coerência entre fins, meios e riscos; capacidade de adaptação; clareza de intenção; compreensão do adversário; consciência de assinaturas; integração logística; ética; e aprendizagem após erro. O oficial deve ser avaliado pela capacidade de pensar sob incerteza, não apenas pela capacidade de repetir doutrina.
- Quinta implicação: o treino deve ser desenhado como laboratório de adaptação. Cada exercício deve conter fricções deliberadas: perda de UAS, degradação de comunicações, falha de logística, alvos falsos, interferência eletromagnética, informação contraditória e decisões legais ou éticas sob pressão. Assim, o treino deixa de ser simples confirmação do plano e passa a testar a capacidade de recomposição. O objetivo não é surpreender artificialmente os oficiais, mas habituá-los a comandar quando a realidade deixa de obedecer ao plano.
- Sexta implicação: o ensino deve integrar *red teaming*. O campo de batalha transparente é uma competição de interpretação. Oficiais devem aprender a pensar como o adversário, a explorar os seus algoritmos, doutrinas, hábitos e limitações. Devem também permitir que adversários simulados ataquem os seus planos, logística, comunicações e pressupostos. *Red teaming* deve obrigatoriamente ser cultura, não evento.

- Sétima implicação: a formação deve treinar decisão com comunicações degradadas. Oficiais devem praticar ordens por intenção, operação sem contacto contínuo, recomposição de C2, mudança de plano sem autorização imediata e uso de comunicações alternativas. Isto desenvolve o comando-missão real. Não basta declarar confiança; é preciso treinar confiança.
- Oitava implicação: a ética e o direito dos conflitos armados devem acompanhar tecnologia. IA, UAS, *targeting* algorítmico e sistemas autónomos levantam problemas de distinção, proporcionalidade, responsabilidade e supervisão humana. A velocidade não elimina o julgamento moral; pelo contrário, torna-o mais difícil e mais necessário. O oficial maduro deve compreender que delegar análise a sistemas não significa delegar responsabilidade. Feldman, Dant e Dreany (2024), Jensen, Whyte e Cuomo (2020) e Kase *et al.* (2022) ajudam a enquadrar estes riscos ao mostrarem que a decisão homem-máquina é simultaneamente uma oportunidade e uma fonte de vulnerabilidade.
- Nona implicação: a formação deve incluir inovação e aquisição. Oficiais superiores e intermédios devem compreender ciclos de desenvolvimento tecnológico, interação com indústria, requisitos mínimos, prototipagem, testes operacionais, segurança de dados e dependência de fornecedores. Num ambiente em que soluções civis podem tornar-se militarmente relevantes em semanas, o oficial não pode ser apenas utilizador final; deve ser interlocutor crítico da inovação.
- Décima implicação: o treino deve ser contínuo e transversal à carreira. A adaptação não pode ficar concentrada num curso específico. A tecnologia deve atravessar cursos de promoção, exercícios de unidades, centros de treino, seminários doutrinários e processos de lições aprendidas. Os oficiais devem regressar periodicamente a ambientes de formação para confrontar experiência acumulada com novas condições técnicas, operacionais e éticas.

Das funções de combate à transformação institucional

Uma forma útil de traduzir os argumentos anteriores é observar os seus efeitos nas principais funções de combate. A tecnologia não afeta apenas uma área isolada; reconfigura simultaneamente comando, informações, fogos, movimen-

to e manobra, proteção, sustentação e influência. O erro seria criar uma “secção de UAS” ou uma “secção de IA” como se a transformação tecnológica fosse uma especialidade externa à força. Pelo contrário, UAS, sensores, dados e guerra eletrônica atravessam todas as funções. A adaptação deve, por isso, ser sistêmica.

- Na função comando, a principal mudança é a passagem de controlo centralizado para coerência descentralizada. O comandante deixa de poder depender de uma imagem perfeita e permanente. Mesmo quando existem *feeds* de UAS e sensores, estes são incompletos, manipuláveis e vulneráveis a interrupção. O comando moderno deve combinar intenção clara, prioridades simples, regras de emissão, critérios de risco e capacidade de recomposição. A autoridade deve ser distribuída antes da crise, porque durante a crise pode ser tarde demais para delegar. A qualidade do comando mede-se menos pela quantidade de ordens emitidas e mais pela capacidade de manter unidade de esforço quando a ligação se degrada.
- Na função informações, a mudança é dupla. Por um lado, há mais dados do que nunca; por outro, há mais risco de erro, saturação e falsa confiança. A abundância de dados não elimina a incerteza. Pode até aumentá-la, porque obriga a decidir que sinais merecem atenção e que padrões são relevantes. A integração de IA permite filtrar e priorizar, mas também pode reproduzir enviesamentos. O ensino militar deve formar oficiais capazes de trabalhar com analistas, questionar fontes, compreender níveis de confiança, interpretar ausência de dados e aceitar que “ver” não é o mesmo que compreender.
- Na função fogos, a ligação sensor-atirador torna-se mais curta e mais distribuída. UAS de pequeno porte podem localizar alvos, corrigir artilharia, atacar diretamente ou alimentar redes de *targeting*. Isto aumenta a letalidade, mas também cria exigências de coordenação. Fogos rápidos sem disciplina podem revelar posições, consumir munições escassas, atingir alvos de baixo valor ou gerar problemas legais. A doutrina deve combinar velocidade com priorização. O alvo mais visível não é necessariamente o mais importante; o alvo mais importante pode não ser juridicamente aceitável; e o alvo aceitável pode não justificar a exposição da plataforma que dispara.
- Na função movimento e manobra, a tecnologia altera a relação entre mobilidade e sobrevivência. Mover-se continua essencial, mas movimento gera

assinatura. Parar permite ocultação, mas também permite deteção por padrões. A manobra deve, por isso, ser intermitente, protegida e sincronizada com efeitos de supressão, guerra eletrónica, decepção e contra-sensores. A velocidade pura não basta. Uma força que avança rapidamente e que é detetada, georreferenciada e atacada pode culminar antes de alcançar o objetivo. A manobra moderna deve criar janelas de oportunidade: momentos limitados em que o adversário está cego, saturado, enganado ou incapaz de reagir.

- Na função proteção, a principal mudança é a passagem da proteção material para a proteção multispectral. Blindagem continua relevante, mas não basta. Proteção inclui reduzir assinaturas térmicas, eletromagnéticas, óticas, digitais e comportamentais. Inclui também camuflagem, dispersão, decepção, mobilidade, contra-UAS, defesas físicas improvisadas, disciplina de luz, controlo de telemóveis, gestão de redes e redundância. O soldado e o oficial devem compreender que qualquer emissão, deslocamento repetido ou concentração temporária comunica algo ao adversário. A proteção moderna é uma forma de comunicação negativa: negar ao inimigo a confiança suficiente para atacar.
- Na função sustentação, a mudança é talvez a mais disruptiva. Logística sempre foi vulnerável, mas agora é mais observável e atacável em profundidade. Isto exige abandonar a ideia de que a eficiência logística máxima é sempre desejável. Grandes depósitos, rotas regulares e centros de manutenção concentrados são eficientes em paz, mas perigosos em guerra. A sustentação moderna deve aceitar redundância, aparente ineficiência e dispersão como preço da sobrevivência. A formação de oficiais deve incluir dilemas logísticos reais: abastecer menos, mas sobreviver mais; dispersar munições, mas dificultar controlo; manter stocks pequenos, mas mais resilientes; aceitar rotas longas para evitar padrões; usar sistemas não tripulados para reduzir exposição humana.
- Na função influência e informação, o campo de batalha transparente cria efeitos políticos imediatos. Imagens de UAS, destruição de viaturas, ataques a civis, falhas logísticas e êxitos táticos circulam rapidamente. A dimensão informacional não é separável da operação. Cada ação tática pode ter efeitos estratégicos. Isto reforça a necessidade de oficiais com consciência política e ética, capazes de compreender que a legitimidade é tam-

bém uma forma de proteção. A tecnologia amplifica tanto êxitos como erros.

A transformação institucional deve alinhar estas funções. Não basta atualizar manuais. É necessário rever exercícios, carreiras, estruturas, incentivos, aquisição, centros de treino e métodos de avaliação. Um exército que ensina o comando-missão mas que promove oficiais que microgerem não se adapta. Uma força que valoriza inovação, mas que pune todos os erros não aprende. Uma força que compra UAS mas não cria operadores, manutenção, doutrina e logística apenas acumula equipamento. Uma força que fala de guerra eletrônica, mas não educa comandantes para compreender o espectro continuará dependente de especialistas.

Esta transformação também exige ligação entre níveis. Ao nível tático, unidades devem treinar sobrevivência, dispersão, contra-UAS e decisão rápida. Ao nível operacional, comandos devem sincronizar efeitos distribuídos, sustentação e campanhas de decepção. Ao nível estratégico, lideranças devem garantir indústria, reservas, aquisição rápida, alianças, interoperabilidade, resiliência civil e legitimidade política. O ensino militar profissional é o local onde estes níveis podem ser articulados, porque permite ao oficial compreender como uma decisão tática se insere num desenho operacional e como este serve fins políticos.

Proposta integrada de adaptação

A transformação descrita pode ser sintetizada em dez linhas de ação. A primeira é doutrinária: reformular a manobra como concentração distribuída de efeitos, não como concentração física de plataformas. A segunda é defensiva: desenvolver defesas avançadas, profundas e ativas que combinem posição, elasticidade tática e fogos de precisão. A terceira é de sobrevivência: transformar dispersão em incerteza física, eletromagnética e cognitiva. A quarta é de comando: criar C2 distribuído, redundante, móvel e baseado em intenção. A quinta é logística: transformar sustentação em manobra, dispersa e protegida.

A sexta linha é tecnológica: integrar UAS, robôs, IA, sensores e contra-UAS em todos os escalões relevantes, evitando tanto fetichismo tecnológico como rejei-

ção conservadora. A sétima é eletromagnética: tornar a guerra eletrónica uma capacidade orgânica de manobra. A oitava é estrutural: criar mecanismos de aquisição rápida, experimentação, adaptação e interação com inovação civil. A nona é cultural: promover iniciativa, diversidade cognitiva, aprendizagem com erro e crítica doutrinária. A décima é educativa: redesenhar o ensino militar profissional para formar julgamento adaptativo, autoconsciência decisional e pensamento estratégico em todos os escalões.

Estas linhas não devem ser vistas como reformas separadas. São interdependentes. Não há logística distribuída sem C2 resiliente; não há manobra com UAS sem guerra eletrónica; não há comando-missão sem educação; não há inovação sem cultura; não há doutrina adaptativa sem vocabulário conceptual; não há concentração de efeitos sem treino de sincronização; não há decisão algorítmica responsável sem ética e julgamento humano.

A principal dificuldade será institucional. Forças militares tendem a adaptar tecnologia mais depressa do que adaptam cultura. É mais fácil comprar UAS do que alterar hábitos de comando; mais fácil criar uma célula de inovação do que reformar processos de avaliação; mais fácil escrever uma nova doutrina do que ensinar oficiais a questionar pressupostos antigos. Por isso, o ensino militar profissional é o mecanismo que liga mudança material a mudança intelectual. Sem educação militar profissional, a tecnologia permanece equipamento. Com educação militar profissional adequada, torna-se capacidade operacional.

Riscos de adaptação incompleta e critérios de implementação

A transformação tecnológica cria também riscos de adaptação incompleta.

- O primeiro risco é a aquisição sem integração. Uma força pode comprar UAS, sensores e sistemas de IA, mas continuar a operar com postos de comando demasiado grandes, comunicações previsíveis, logística centralizada e processos de decisão excessivamente dependentes de aprovação superior. Nesse caso, a tecnologia aumenta a superfície de exposição sem alterar a lógica operacional. O UAS torna-se mais uma ferramenta num modelo antigo, não um elemento de transformação. A integração deve ser avaliada não pelo número de sistemas adquiridos, mas pela sua incorpora-

ção em exercícios, doutrina, logística, manutenção, treino de operadores, cadeias de dados, regras de empenhamento e processos de decisão.

- O segundo risco é a ilusão de velocidade. A compressão da cadeia sensor-atirador pode levar à ideia de que decidir mais depressa é sempre decidir melhor. Henâker (2022) mostra que estilos de decisão rápidos podem ter vantagens em contextos de combate, mas a velocidade sem adaptação pode produzir impulsividade. Uma boa decisão não se mede apenas pela rapidez, mas pela qualidade do processo e pela adequação ao contexto. No campo de batalha moderno, a rapidez é necessária para sobreviver e explorar oportunidades; porém, a velocidade deve ser disciplinada por intenção, ética, compreensão do adversário e avaliação de risco. O ensino militar deve, por isso, treinar a distinção entre decisão rápida, decisão precipitada e decisão oportunamente deliberada.
- O terceiro risco é a centralização por excesso de informação. A transparência do campo de batalha pode seduzir escalões superiores a intervir em decisões táticas, porque “veem” mais do que antes. Contudo, mais informação não significa melhor compreensão. A microgestão de unidades dispersas pode atrasar decisões, aumentar emissões, reduzir iniciativa e criar dependência. O paradoxo é que tecnologias que permitem ver mais podem enfraquecer o comando-missão se forem usadas para controlar mais. A adaptação cultural deve preservar a iniciativa subordinada e limitar a tentação de transformar a consciência situacional superior em interferência permanente.
- O quarto risco é a dependência tecnológica. Sistemas digitais podem falhar, ser enganados, ficar sem energia, perder ligação, ser comprometidos por ciberataques ou tornar-se inúteis por guerra eletrónica. O oficial moderno deve saber operar com tecnologia, mas também sem ela. Isto implica treino analógico, mapas físicos, messageiros, sinais visuais, procedimentos de *fallback*, comunicações de baixa potência, redundância de navegação e capacidade de estimativa sem sensores perfeitos. A tecnologia deve aumentar a resiliência e não substituí-la.
- O quinto risco é a homogeneidade cognitiva. Se todos os oficiais forem formados nos mesmos modelos, com os mesmos *datasets*, os mesmos simuladores e as mesmas respostas doutrinárias, os sistemas de IA podem amplificar pressupostos errados. Sookermany (2016) valoriza diversidade

e pluralidade precisamente porque o imprevisível exige múltiplas formas de ver e interpretar. O ensino e formação militares deve, por isso, incluir debate, dissenso profissional, *red teaming* e confronto com perspetivas externas. A crítica não deve ser entendida como indisciplina, mas como ferramenta de robustez intelectual.

Daqui decorrem alguns critérios de implementação. Primeiro, cada nova tecnologia deve ser acompanhada por uma pergunta doutrinária: que conceito operacional altera ou exige? Segundo, cada alteração doutrinária deve ser acompanhada por uma pergunta organizacional: que estrutura, especialidade, processo ou autoridade precisa de mudar? Terceiro, cada mudança estrutural deve ser acompanhada por uma pergunta educativa: que competências devem ser ensinadas, treinadas e avaliadas? Quarto, cada inovação deve ser testada contra um adversário adaptativo, e não apenas demonstrada em condições favoráveis. Quinto, cada lição aprendida deve ser transformada em aprendizagem institucional: doutrina revista, treino ajustado, currículo atualizado e incentivos alinhados.

A formação do oficial no centro da transformação

A formação de oficiais com alguma maturidade merece especial atenção porque estes oficiais ocupam frequentemente posições de charneira. Não são apenas executantes de tática nem apenas formuladores de política; traduzem orientações estratégicas em planos operacionais, supervisionam treino, comandam unidades, avaliam risco, aconselham superiores e moldam a cultura dos subordinados. Se estes oficiais não compreenderem a transformação tecnológica e doutrinária, a instituição pode adquirir meios novos sem alterar práticas antigas.

O oficial maduro deve ser formado como intérprete da mudança. Isso exige três competências complementares. A primeira é competência conceitual: compreender as transformações do campo de batalha, distinguir tendências duradouras de modas tecnológicas e reformular conceitos clássicos. A segunda é competência prática: saber planear operações com UAS, guerra eletrónica, logística distribuída, C2 degradado e fogos de precisão. A terceira é competência

pedagógica: ser capaz de transmitir às suas unidades uma cultura de aprendizagem, disciplina de assinatura, iniciativa subordinada e adaptação contínua.

A experiência deste oficial deve ser usada como matéria-prima de aprendizagem. Em vez de lhe apresentar apenas novas “lições” a memorizar, o ensino e formação militares devem colocá-lo perante dilemas que obriguem a comparar experiência passada com condições novas. Um exercício pode pedir que planeie uma operação de brecha com métodos tradicionais e depois introduzir ISR persistente, UAS FPV, minas, guerra eletrónica e logística vulnerável. Outro pode simular a perda do posto de comando e obrigar subordinados a continuar a missão. Outro pode introduzir um sistema de IA que recomenda um alvo juridicamente duvidoso, exigindo decisão ética sob pressão temporal. O objetivo é criar fricção intelectual, não apenas confirmar doutrina.

A maturidade profissional também implica humildade. O oficial experiente pode sentir que já viu variações suficientes da guerra para confiar no seu padrão habitual. Contudo, a guerra moderna combina elementos antigos e novos de forma desconcertante: trincheiras e IA, minas e UAS, artilharia massiva e software, blindagem e robótica, propaganda e *targeting* algorítmico. A função do ensino militar profissional é precisamente impedir que a experiência se transforme em rigidez. O ensino e formação militares não desvaloriza a experiência; obriga-a a dialogar com a novidade.

O oficial maduro deve ainda ser formado como treinador de adaptação. A sua responsabilidade não termina quando compreende a mudança; começa quando consegue transformá-la em treino para a unidade. Isso implica desenhar exercícios realistas, criar critérios de avaliação, promover análise pós-ação honesta e corrigir hábitos perigosos, como a concentração excessiva, o uso previsível de comunicações, a dependência de GPS ou a logística demasiado centralizada. O oficial é, por isso, multiplicador institucional da aprendizagem.

Por fim, o oficial maduro deve ser preparado para liderar mudança institucional. A adaptação não ocorre apenas no campo de tiro ou no simulador. Ocorre em reuniões de planeamento, processos de aquisição, revisões doutrinárias, relatórios de lições aprendidas, seleção de instrutores, desenho de exercícios e avaliação de desempenho. Oficiais intermédios e superiores decidem o que é premiado, tolerado ou ignorado. Se valorizarem apenas conformidade, a organização repetirá procedimentos. Se valorizarem aprendizagem disciplinada, a

organização adaptar-se-á. Neste sentido, o ensino e formação militares é um instrumento de transformação institucional porque forma aqueles que irão ensinar, avaliar e comandar a próxima geração.

Um modelo pedagógico para a adaptação contínua

A partir dos textos analisados, pode propor-se um modelo pedagógico assente em quatro ciclos: compreender, experimentar, decidir e refletir. O primeiro ciclo, compreender, corresponde à construção de literacia conceptual e tecnológica. Nele, o oficial estuda doutrina, história militar, tecnologia emergente, guerra eletrónica, logística, IA, ética e cultura estratégica. O objetivo não é acumular informação, mas construir categorias de análise. Sem categorias adequadas, a força observa fenómenos novos com linguagem antiga e tende a interpretá-los mal.

O segundo ciclo, experimentar, deve ocorrer em simuladores, *wargames*, exercícios de campo e laboratórios de inovação. O oficial deve ser exposto a cenários em que a tecnologia funciona parcialmente, falha inesperadamente ou produz efeitos ambíguos. Um cenário pode oferecer superioridade de UAS no início e perdê-la por *jamming* a meio da operação. Outro pode obrigar a dispersar logística e, em seguida, enfrentar uma oportunidade que exige concentração rápida de munições. Outro pode introduzir informações contraditórias provenientes de sensores, fontes humanas e análise algorítmica. Estes exercícios devem colocar em tensão princípios que, em sala de aula, parecem compatíveis: dispersão e controlo, velocidade e validação, proteção e missão, sigilo e coordenação, eficiência e redundância.

O terceiro ciclo, decidir, deve obrigar o oficial a assumir responsabilidade. A educação militar profissional não pode transformar-se apenas em debate académico. O comandante deve decidir com tempo limitado, informação incompleta e consequências. Isto é particularmente importante para oficiais maduros que poderão ter desenvolvido prudência excessiva ou dependência de processos formais. O estudo de Henåker (2022) é útil precisamente porque mostra que a dependência decisória pode prejudicar desempenho em ambiente competitivo. O ensino deve treinar o oficial para pedir aconselhamento quando necessário, mas sem abdicar da decisão.

O quarto ciclo, refletir, é o que transforma experiência em aprendizagem. A análise pós-ação deve ir além da pergunta “ganhámos ou perdemos?”. Deve perguntar: que pressupostos orientaram a decisão? Que sinais foram ignorados? Que parte do plano resistiu à fricção? Que dependência tecnológica se revelou perigosa? Que emissões denunciámos? Que alternativa logística teria aumentado a sobrevivência? Que momento exigia descentralização? Que erro decorreu de cultura organizacional e não de incompetência individual? Esta reflexão aproxima-se da desconstrução defendida por Sookermany (2016): desmontar significados para reconstruir julgamento.

Este modelo pedagógico deve ser cumulativo. Um curso isolado sobre UAS ou IA não basta. A tecnologia deve atravessar todo o percurso formativo. Num módulo de logística, deve discutir-se vigilância por UAS e rotas dispersas. Num módulo de liderança, deve discutir-se decisão sob perda de C2. Num módulo de ética, deve discutir-se *targeting* algorítmico. Num módulo de história militar, deve comparar-se a crise da manobra na Primeira Guerra Mundial com os obstáculos contemporâneos criados por ISR e fogos de precisão. Num módulo de operações, deve exigir-se integração de guerra eletrônica, contra-UAS, fogos e sustentação.

A formação de oficiais maduros deve ainda incluir contacto com atores externos. Universidades, empresas tecnológicas, centros de investigação, indústria de defesa, especialistas em ciber, analistas de dados e operadores de UAS civis podem desafiar a visão institucional. Isto não significa militarizar a universidade ou civilizar a guerra, mas reconhecer que a fronteira entre inovação civil e militar se tornou mais porosa. O oficial deve ser capaz de dialogar com estes atores sem perder critérios militares, éticos e políticos.

Finalmente, o ensino e formação militares deve criar uma cultura de escrita profissional. A adaptação doutrinária exige oficiais capazes de escrever lições aprendidas, criticar conceitos, propor alterações e comunicar ideias com precisão. O vocabulário é uma ferramenta de transformação. Quando uma instituição não consegue nomear um problema, dificilmente consegue resolvê-lo. Escrever sobre dispersão como incerteza, logística como função exposta, guerra eletrônica como condição de manobra ou IA como mediação de decisão ajuda a converter experiência dispersa em conhecimento institucional.

Conclusão

A nossa conclusão fundamental é a de que a tecnologia muda o carácter da guerra, mas são as instituições que decidem se essa mudança se transforma em vantagem. As forças militares que apenas acrescentarem UAS, IA ou robôs a estruturas antigas poderão tornar-se mais visíveis, mais dependentes e mais vulneráveis. As forças que integrarem tecnologia com doutrina, cultura, estrutura, ensino e treino poderão sobreviver, adaptar-se e impor dilemas ao adversário. O centro da transformação não está, portanto, apenas no sistema tecnológico, mas no julgamento profissional dos oficiais que o empregam, ensinam e treinam.

A tecnologia alterou o campo de batalha moderno ao torná-lo mais transparente, letal, rápido e interligado. UAS, IA, sensores, guerra eletrónica, robótica e fogos de precisão tornam arriscada a concentração física, expõem a logística, comprimem ciclos de decisão, vulnerabilizam postos de comando e fragilizam doutrinas assentes em liberdade de movimento presumida. No entanto, esta transformação não significa o fim da doutrina, da manobra, da blindagem ou da decisão humana. Significa que todas estas dimensões precisam de ser reformuladas.

A guerra de manobra permanece relevante se for adaptada ao novo ambiente. A manobra futura deverá concentrar efeitos sem concentrar vulnerabilidades, operar com forças dispersas, mas coerentes, integrar UAS e robôs, degradar sensores adversários, manipular assinaturas, proteger logística, usar guerra eletrónica como condição de movimento e aceitar que a surpresa pode depender mais da confusão do adversário do que da invisibilidade própria. A defesa posicional também regressa, mas não como defesa passiva; regressa como defesa avançada, profunda e ativa, capaz de explorar a dificuldade contemporânea de atravessar o campo de batalha intacto.

As adaptações necessárias são doutrinárias, operacionais, culturais e estruturais. Doutrinariamente, é preciso redefinir massa, dispersão, proteção, manobra e sustentação. Operacionalmente, é necessário reorganizar C2, logística, engenharia, guerra eletrónica e contra-UAS. Culturalmente, é preciso valorizar iniciativa, aprendizagem, experimentação e crítica. Estruturalmente, é necessário aproximar forças armadas, indústria, tecnologia civil e processos de aquisição rápida, sem perder controlo estratégico e ético.

O ensino, a formação e o treino militares são decisivos porque formam o tipo de oficial capaz de conduzir esta adaptação. A formação de oficiais com maturidade deve transformar experiência em julgamento adaptativo. Deve libertar o oficial de pressupostos herdados, treiná-lo para desconstruir doutrinas, desenvolver vocabulário para novos fenómenos, praticar decisão sob pressão, cultivar intuição profissional, compreender tecnologia sem se submeter a ela e comandar por intenção em ambientes degradados. O treino, por sua vez, deve transformar estes princípios em proficiência operacional, expondo oficiais e unidades a fricções realistas e exigindo recomposição após falha.

Bibliografia

- Biddle, S. (2004). *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press.
- Buchholz, B. (2025). Dispersion as uncertainty: Rethinking survivability in the era of ISR-enabled targeting. *Military Review Online Exclusive*, December 2025.
- Caron, J.-F. (2026). Military drones: A thousand snipers in the air. Is the Russo-Ukrainian War a tactical and technological inflection point in the history of warfare? *The Journal of Slavic Military Studies*. <https://doi.org/10.1080/13518046.2026.2666977>
- Chamayou, G. (2015). *A Theory of the Drone*. The New Press.
- Clausewitz, C. von. (1984). *On War* (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press.
- Feldman, P., Dant, A., & Dreany, H. (2024). War elephants: Rethinking combat AI and human oversight. *arXiv*. <https://doi.org/10.48550/arXiv.2404.19573>
- Freedman, L. (2005). A theory of battle or a theory of war? *Journal of Strategic Studies*, 28(3), 425–435. <https://doi.org/10.1080/01402390500137275>
- Henåker, L. (2022). Decision-making style and victory in battle: Is there a relation? *Comparative Strategy*, 41(4), 415–436. <https://doi.org/10.1080/01495933.2022.2087436>
- Jensen, B. M., Whyte, C., & Cuomo, S. (2020). Algorithms at war: The promise, peril, and limits of artificial intelligence. *International Studies Review*, 22 (3), pp. 526-550. <https://doi.org/10.1093/isr/viz025>
- Kase, S. E., Hung, C. P., Krayzman, T., Hare, J. Z., Rinderspacher, B., & Su, S. M. (2022). The future of collaborative human-artificial intelligence decision-ma-

- king for mission planning. *Frontiers in Psychology*, 13, pp. 1-8. <https://doi.org/10.3389/fpsyg.2022.850628>
- King, A. (2026). *AI, Automation, and War: The Rise of a Military-Tech Complex*. [Obra discutida em recensão de Sarah Chapman Trim].
- Lingel, S., Hagen, J., Hastings, E., Lee, M., Sargent, M., Walsh, M., & Blancett, D. (2020). *Joint All-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications*. RAND Corporation.
- Marcella, G. (Ed.). (2010). *Teaching Strategy: Challenge and Response*. Strategic Studies Institute, U.S. Army War College.
- Milevski, L. (2024). Manoeuvre warfare in the Baltic: Political imperatives and tactical conditions. *The RUSI Journal*, 169 (6), pp. 78-86. <https://doi.org/10.1080/03071847.2024.2407534>
- Sookermany, A. M. (2016). Military education reconsidered: A postmodern update. *Journal of Philosophy of Education*. <https://doi.org/10.1111/1467-9752.12224>
- Strawser, B. J. (2010). Moral predators: The duty to employ uninhabited aerial vehicles. *Journal of Military Ethics*, 9 (4), pp. 342-368.
- Taylor, C. (2025). The coming blitzkrieg: Adapting armored formations for the future of warfare. *Military Review Online Exclusive*, December 2025.
- Trim, S. C. (2026). AI, automation, and war: The rise of a military-tech complex [Review]. *The RUSI Journal*, 171(3), pp. 124-125. <https://doi.org/10.1080/03071847.2026.2652186>
- Wu, C.-S. (2026). Rethinking warfare in the AI era: The Modern System, asymmetric conflict and Taiwan's cross-strait security. *Defence Studies*. <https://doi.org/10.1080/14702436.2026.2671057>



CAPÍTULO DECIMOTERCERO

URUGUAY. CENTRO DE ALTOS ESTUDIOS NACIONALES (CALEN)

La influencia de las nuevas tecnologías en los escenarios de operaciones futuras, implicancias desde la perspectiva del Colegio de Defensa del Uruguay -CALEN

Alfonso Fojo

Resumen: Las nuevas tecnologías, como la Inteligencia Artificial, los sistemas autónomos de defensa, la computación cuántica, y la presencia de nuevos dominios como el ciberespacial, están reconfigurando los entornos para el empleo del instrumento militar hacia la consecución de los objetivos estratégicos de los Estados.

No es ninguna novedad de que los conflictos se vienen reconfigurando, pudiéndose describir como hiperconectados y presentes tanto en dominios físicos como no físicos, desarrollándose entornos caracterizados como volátiles, inciertos, complejos y ambiguos (VUCA) y que se perciben como: Frágiles¹, Ansiosos, No lineales e Incomprensibles (BANI²).

Desde la perspectiva del Colegio de Defensa de Uruguay, en la que su actor de referencia es el Estado uruguayo; el cual, considerando estas transformaciones

¹ Brittle: Los sistemas pueden romperse o colapsar de manera repentina. Anxious: Genera incertidumbre, estrés y miedo constante a tomar decisiones equivocadas. Non-linear: Las causas y los efectos están desconectados; pequeñas acciones pueden generar consecuencias desproporcionadas. Incomprehensible:

² Acuñado en 2020 por Jamais Cascio, en su artículo "Facing the Age of Chaos, tratando con ello caracterizar el ambiente estratégico desde la percepción.

tecnológicas como claras señales de hechos portadores de futuro, nos ponen en alerta y a la vez nos comunican la necesidad de adaptar y o reconfigurar capacidades en función de la salvaguarda de los intereses nacionales vitales para el sujeto estratégico de referencia ya mencionado.

El presente artículo analiza el impacto de estas tecnologías en los escenarios futuros desde un enfoque cualitativo y prospectivo. Asimismo, examina sus posibles implicancias estratégicas desde la perspectiva del Colegio de Defensa del Uruguay, considerando las limitaciones existentes; arribando a conclusiones que marcan como principal desafío, la capacidad de adaptación e integración tecnológica en torno al desarrollo de capacidades las cuales habilitarían al actor de referencia a enfrentar los desafíos futuros y contribuir al logro del bien común.

Palabras clave: Entornos operativos futuros, Nuevas tecnologías, Disruptivas, Emergentes.

Acerca del autor: Alfonso Fojo, Coronel del Arma de Infantería. Magister en Estrategia Nacional por el Centro de Altos Estudios Nacionales (CALEN). Cursó el Posgrado de Inteligencia Estratégica en el CALEN. Es docente en dicho instituto de Estrategia, Prospectiva y Planificación Estratégica

Introducción

La tecnología aplicada ha sido históricamente un factor determinante en la transformación de cómo se emplea el instrumento militar asociado a un fin dado.

El concepto de guerra de maniobra, si bien fue conceptualmente concebida antes de la primera guerra mundial, no se pudo llevar a la práctica hasta la segunda guerra mundial en función de que no se contaba con las capacidades tecnológicas necesarias, por lo que no fue hasta que el desarrollo tecnológico maduró lo suficiente, que el concepto pudo ser llevado a la práctica en un contexto de guerra real. Actualmente vemos como las tecnologías disruptivas emergentes van más delante de los conceptos.

No es ninguna novedad, afirmar que en las últimas dos décadas se identifica una aceleración en la materialización de nuevas tecnologías las cuales no solo afecta a los medios, sino que también a los procesos de decisión, a la organización, y a la naturaleza del conflicto por lo tanto resulta en una Revolución en los Asuntos Militares³, a toda regla.

Estas transformaciones tecnológicas⁴ generan mutaciones tanto en la forma en que se conceptualizan, planean y llevan adelante las operaciones, ergo transformando los entornos operativos, ya sea complejizándolos, modificando el ritmo de las operaciones y o aumentando las interconexiones.

En este sentido Gray C. (The strategy bridge: Theory for practice, 2010) afirma que los escenarios contemporáneos se caracterizan por su condición multidominio, donde convergen los ámbitos físico y no físico. Estas nuevas realidades impactan en las transformaciones de los medios utilizados, en el tipo de conflicto (Zona Gris por ejemplo), en el dominio (Aéreo, Terrestre, Cognitivo, espacial ciber, etc.), los procesos de toma de decisiones, las estructura y organización del instrumento militar, las normas jurídicas, la interacción entre actores, entre otros.

Ya (Clausewitz, 1832) nos decía que la guerra era un entorno caótico caracterizado por la fricción el azar y la incertidumbre.

Por lo que otras de las características de los entornos operativos serian la creciente incertidumbre ya sea debido al exceso informacional y la desinformación o bien las lagunas de información en particular sobre aspectos críticos

El hecho de que las Tecnologías emergentes se encuentren en evolución, se interconecten y se integren entre ellas, es un elemento clave a la hora intentar medir el impacto, ergo comprender el sistema e identificar el problema en

³ RMA: Revolution in Military Affairs es un concepto que describe cambios fundamentales en la forma de empleo del instrumento militar, dicho cambio es consecuencia de la incorporación de nuevas tecnologías combinadas con transformaciones en la doctrina, organizacionales y operativas.

⁴ Como la inteligencia artificial, los sistemas autónomos, la guerra cibernética el análisis avanzado de datos, el ciberespacio y las tecnologías de la información y las comunicaciones

cuestión y realizar un correcto diagnóstico enfocado a la toma de decisiones informada.

En este sentido, conceptos clásicos como el control, la superioridad de la información y la coordinación requerirán de la adecuada revisión, surgiendo además dilemas éticos estratégicos.

En consecuencia, comprender el alcance y las implicancias de estas tecnologías resulta fundamental para anticipar la reconfiguración de los escenarios futuros y además para orientar procesos de planificación y vigilancia del entorno de forma más eficaces.

Abordaje metodológico⁵

En este contexto, el presente trabajo tiene como objetivo analizar la influencia de las nuevas tecnologías e impactos asociados a los escenarios de operaciones futuras y evaluar con particular atención las implicaciones para la República Oriental del Uruguay, particularmente aquellos asociados con los Intereses nacionales vitales⁶ y los Objetivos Estratégicos del Estado.

Para ello se empleó un abordaje analítico y prospectivo sustentado en la revisión de literatura académica y documentos especializados de forma de identificar posibles escenarios futuros -con consciencia del que el fallo prospectivo es un hecho⁷-, que permiten sugerir unas necesidades de capacidades asociada a unas EDT y conceptos, entre otras implicancias estratégicas.

Por lo que, en opinión del autor, el artículo aportará conocimiento instrumental al actor de referencia del CALEN y a la ACDIA, particularmente en aspectos de adaptación organizacional frente a la evolución tecnológica en el marco de un entorno VUCABANI.

⁵ Función: plantear el problema y justificar el estudio

⁶ Estos según Uruguay (2020) representan la más alta prioridad de una nación en relación con su supervivencia, desarrollo, crecimiento, y bienestar de su población.

⁷ Los Cisnes Negros que según (Taleb, 2007) son eventos altamente improbables, difíciles de prever y de gran impacto.

El presente Análisis documental es de tipo y con enfoque descriptivo cualitativo, exploratorio, utilizando como técnicas y fuentes de información la revisión bibliográfica, análisis documental y consulta a expertos⁸.

Limitaciones al Estudio

Se identifican o reconocen las siguientes limitaciones del estudio:

- Abordar el análisis desde la perspectiva del Estado uruguayo introduce un sesgo de enfoque.
- El cambio tecnológico exponencial aumenta la incertidumbre inherente a los estudios prospectivos, siendo el fallo prospectivo una posibilidad reconocida.
- Se reconocen que habrá información a la que el autor no accede debido a restricciones de acceso a información clasificada.
- Posible sobredimensionamiento en el impacto de tecnologías analizadas.

Para la redacción del trabajo se situó en trabajo en el nivel Político Estratégico:

- Describiendo las nuevas tecnologías clave.
- Identificando posibles impactos operativos.
- En función de ellos infiriendo unas implicaciones y desafíos para Uruguay.

Las nuevas tecnologías, además de reconfigurar el entorno operativo, se presentan como potentes integradores de “diversos sistemas” potenciando además otras capacidades ya presentes en los instrumentos militares de los Estados, posicionándose como una ventaja estratégica significativa en los entornos operativos futuros.

Es en este marco, se analizó las implicancias para la República Oriental del Uruguay, prestando particular consideración a su modelo de defensa, sus ca-

⁸ Se consultó a los integrantes de la Cátedra del área científico tecnológico del Centro de Altos estudios Nacionales de la ROU

pacidades, debilidades estructurales y retos a futuro, considerando además como se alinea con la acción exterior del Estado y su inserción internacional.

El artículo se estructura de la siguiente manera: primariamente, se presenta el marco metodológico y teórico conceptual el cual dará sustento al análisis; seguidamente se desarrolla el análisis y discusión sobre el impacto de las nuevas tecnologías en los entornos operatorios futuros; finalmente, conclusiones y en función de ellas algunas recomendaciones.

Marco teórico y conceptual

Marco teórico

El análisis de impacto de las EDT en el entorno operativo parte de la premisa que no todo cambia al mismo ritmo, y como bien señalaba Clausewitz C. (De la guerra, 1832) se puede diferenciar entre la naturaleza y el carácter de la guerra⁹, siendo para este caso de análisis los entornos operativos.

La naturaleza de la guerra está marcada por la violencia, la incertidumbre y su dimensión política. Esta naturaleza permanece constante a lo largo del tiempo. Ahora bien, en lo que refiere a su carácter a diferencia de la anterior, este sí evoluciona, estando influido por factores como la tecnología, la organización y el contexto histórico.

Según Gray, C. (The strategy bridge: Theory for practice, 2010) la tecnología no cambia la esencia de la guerra, pero sí transforma profundamente la manera en que se lleva a cabo. Es decir, no alcanza con incorporar nuevas herramientas: su verdadero impacto depende de cómo se integran en la doctrina, en la estrategia y en la forma de pensar el empleo de la fuerza.

⁹ En este caso se asocia exclusivamente al uso del instrumento militar, pero en una visión más integral se pueden incluir los instrumentos del poder nacional. Por ejemplo a través del marco DIME: Diplomático, informacional, militar y económico. Si bien podemos encontrar otros marcos más abarcativo como el MIDFIELD por: Militar, informacional, diplomático, financiero, inteligencia, económico, legal y desarrollo.

Así mismo, (Freedman, 2013) plantea que el empleo del instrumento militar es un proceso adaptativo continuo por lo que en ambientes caracterizados como VUCABANI.

En este sentido según Alvez W. la innovación tecnológica y en particular las EDT presenta múltiples desafíos, abriendo a la vez nuevas oportunidades y amenazas y a la vez introduce grandes niveles de incertidumbre (Comunicación personal, 2026).

En este contexto, la ventaja no radica solo en disponer de tecnología avanzada, sino en la capacidad de comprenderla, interpretarla, regularla y aprovecharla antes que el resto de los actores presentes en el entorno, en particular contra aquellos que no comparten los objetivos del sujeto estratégico considerado – el Estado-.

Finalmente, pero no menos importantes autores como Kilcullen (Out of the mountains: The coming age of the urban guerrilla., 2013) han puesto el foco en un aspecto cada vez más relevante como lo es el entorno informacional o cognitivo -.

En la actualidad la lisa estratégica no se limita solo al terreno físico (tierra, mar, aire, espacio), al que también se suman el virtual (ciberespacio / espectro electromagnético), sino que se extiende al ámbito de las percepciones, las narrativas y la influencia sobre la opinión y la popular “infosfera”¹⁰ que Alvin Toffler acuña en su libro la tercera ola (La Tercera Ola, 1979), donde la información se convierte en un instrumento central del poder.

Marco conceptual

Con nuevas tecnologías nos referiremos lo que se conoce como tecnologías emergentes disruptivas¹¹ (y o críticas). Si bien no hay una definición consensuada, la NATO se refiere a ellas como las “*Technologies that are radically changing the way wars are fought and societies operate*” (NATO, 2026) por su

¹⁰ Infoesfera: Ámbito donde interactúan datos, humanos, algoritmos y tecnologías, difuminando lo físico, lo digital e informacional.

¹¹ Emerging and Disruptive Technologies (EDTs)

parte el Reino Unido de Gran Bretaña la define como “*Technologies that have the potential to significantly alter the way people live, work, fight and interact*” (UK, 2018).

A los efectos del presente artículo las EDT serán las “tecnologías o desarrollos tecnológicos capaces de producir transformaciones profundas y aceleradas en los ámbitos políticos, económicos, psicosociales y Militares, modificando estructuras y generando oportunidades y amenazas estratégicas”.¹²

Según (Rahman, 2024) las EDT se caracterizan por ser tecnologías que se encuentran en una fase de maduración acelerada y que en algunos casos aún no han desarrollado su máximo potencial o no sabemos cómo pueden llegar a transformarse. Siendo entonces sus características clave diferenciadoras el ser novedades¹³, presentar un rápido crecimiento¹⁴, tener un gran Impacto¹⁵ y existe incertidumbre de su deriva¹⁶.

Según (NATO, 2026), estas se agrupan en áreas clave como:

- Inteligencia Artificial (IA): Para el análisis masivo de datos y toma de decisiones rápida.
- Sistemas Autónomos: Drones comerciales modificados
- Tecnologías Cuánticas: Para comunicaciones seguras o detección de submarinos.
- Espacio: El uso de constelaciones de satélites de órbita baja (LEO) para vigilancia persistente.
- Biotecnología y Mejora Humana.
- Datos y Computación en la Nube.

El (World Economic Forum, 2026) señala como tecnologías disruptivas a la Inteligencia artificial, la Computación cuántica, la Biotecnología y genética, el In-

¹² Elaboración propia basada en las definiciones mencionadas y el Marco teórico que adopta en CALEN con propósitos académicos.

¹³ Pueden ser invenciones completamente nuevas o aplicaciones novedosas de tecnologías ya existentes.

¹⁴ Normalmente evolucionan y mejoran a un ritmo acelerado.

¹⁵ Tienen el potencial de revolucionar industrias existentes y crear nuevas.

¹⁶ Sus efectos a largo plazo pueden ser difíciles de predecir.

ternet de las cosas¹⁷, los Vehículos autónomos, Blockchain los Nuevos materiales y Nanotecnología

Como se observa no hay unanimidad, pero si muchas coincidencias en este sentido, y por poner otro ejemplo para (Australian Strategy Policy Institute, 2023) las tecnologías críticas o claves debido a su impacto a futuro en los entornos de la seguridad, la defensa, la economía y la competencia geopolítica global son:

Materiales avanzados y manufactura encontrándose en ellos

- Materiales y manufactura a nano escala.
- Recubrimientos avanzados.
- Materiales inteligentes.
- Materiales compuestos avanzados.
- Metamateriales novedosos.
- Procesos de mecanizado de alta precisión.
- Explosivos y materiales energéticos avanzados.
- Extracción y procesamiento de minerales críticos.
- Imanes avanzados y superconductores.
- Protección avanzada.
- Síntesis química de flujo continuo.
- Manufactura aditiva (impresión 3D).

Inteligencia artificial, computación y comunicaciones

- Comunicaciones avanzadas por radiofrecuencia (5G y 6G).
- Comunicaciones ópticas avanzadas.
- Algoritmos de inteligencia artificial y aceleradores de hardware.
- Tecnologías de registros distribuidos (Blockchain).

¹⁷ Internet of the Things (IoT)

- Analítica avanzada de datos.
- Aprendizaje automático (Machine Learning).
- Tecnologías de ciberseguridad defensiva.
- Computación de alto rendimiento.
- Diseño y fabricación avanzada de circuitos integrados.
- Procesamiento de lenguaje natural.

Energía y medio ambiente

- Hidrógeno y amoníaco para generación de energía.
- Super capacitores.
- Baterías eléctricas.
- Energía fotovoltaica.
- Gestión y reciclaje de residuos nucleares.
- Tecnologías de energía dirigida.
- Biocombustibles.
- Energía nuclear.

Tecnologías cuánticas

- Computación cuántica.
- Criptografía postcuántica.
- Comunicaciones cuánticas.
- Sensores cuánticos.

Biotecnología y vacunas

- Biología sintética.
- Manufactura biológica.
- Vacunas y contramedidas médicas.

Sensores, navegación y temporización

- Sensores fotónicos.

Defensa, espacio, robótica y transporte

- Motores aeronáuticos avanzados e hipersónicos.
- Drones, enjambres y robots colaborativos.
- Pequeños satélites.
- Tecnologías de operación de sistemas autónomos.
- Robótica avanzada.
- Sistemas de lanzamiento espacial.

Cabe destacar que el informe destaca que las tecnologías serán determinantes para la multiplicación del poder y la competitividad geopolítica a futuro.

Entorno Estratégico Global

Según NATO (Strategic Concept, 2022) en su descripción del entorno estratégico expresa que el terrorismo en sus múltiples manifestaciones ha expandido sus redes, mejorado sus capacidades e invertido en nuevas tecnologías para mejorar su alcance y letalidad.

Así mismo expresa que Competidores estratégicos y o posibles adversarios están invirtiendo en tecnologías que podrían llegar a restringir el acceso y libertad para operar en el espacio, degradar las capacidades espaciales y atacar infraestructura civil y militar.

Expresa además que las tecnologías emergentes y disruptivas han modificado el entorno operativo adquiriendo mayor relevancia, convirtiéndose estas EDT en objeto e instrumento de competencia global, debido a la creciente correlación de estas tecnologías con capacidades críticas particularmente en los entornos operativos futuros.

En el reciente reporte del Foro Económico Mundial (Global Risks Report , 2026) se identifican 33 *“risk that is most likely to present a material crisis on a global*

scale in 2026", de los cuales 6 estarían en el marco de las tecnologías. Ellas son:

- La falta de información y desinformación.
- Resultados adversos derivados de la IA¹⁸.
- La inseguridad cibernética.
- Los censores y vigilancia.
- Los resultados adversos de tecnologías nuevas /emergentes.
- Daños en línea.



Figura 1. Riesgo que probablemente suponga una crisis material a escala global en 2026. Nota: Extraído de (World Economic Forum, 2026)

¹⁸ En el tiempo presente

Dicho informe a “resultados adversos derivados de la IA” como riesgos severos que más crecen en el largo plazo, manteniéndose la severidad por la falta de información y la desinformación.



Figura 2. Riesgo Global ponderado por Gravedad, en el corto plazo (2 años) y largo plazo (10 años). Nota: Extraído de (World Economic Forum, 2026)

Tales afirmaciones se basan en que esta tecnología potencia la desinformación, ya que habilita amplificación de la desinformación mediante la manipulación de información y el uso de algoritmos basados en Bigdata lo cual termina erosionando la confianza en las instituciones democráticas.

Esta EDT en combinación con otras tecnologías como la automatización podría llegar a generar disrupción del empleo, por ejemplo, en el transporte donde el transporte autónomo ya llegó para quedarse.

En las capacidades militares se ve reflejado claramente con los sistemas autónomos de targeting y toma de decisiones en el conflicto de IRAN, en los aspectos vinculados a la democracia como votaciones manipuladas u operaciones de influencia basada en algoritmos utilizando Bigdata.

Las Tecnologías de la información y ecosistema digital además de las lagunas de información la desinformación y la inseguridad en el entorno Cibernético, en el informe colocan a la desinformación en el puesto 2 y la ciberseguridad en el top 10 en el corto plazo.

Por lo dicho anteriormente se identifica como posible la manipulación electoral y la polarización y debido a ella la fragmentación, los ataques a infraestructuras críticas y una posible pérdida de control sobre la narrativa pública. Estos fenómenos corroen el discurso público y debilitan la respuesta a crisis.

Características de la República Oriental del Uruguay (ROU)

La ROU se caracteriza por su neutralidad, con un instrumento militar modesto y con una concepción estratégica de empleo eminentemente defensivo-disuasoria¹⁹

En Uruguay se identifican algunas limitaciones estructurales como la pequeña escala, limitados recursos y peso geopolítico reducido. Si bien cuenta con una gran estructura de capacitación en el ámbito de la ciencia y la tecnología siendo la Agencia de gobierno electrónico y sociedad de la información del conocimiento (AGESIC), Administración Nacional de Telecomunicaciones (ANTEL) y la Universidad tecnológica (UTEC) referentes en este sentido.

AGESIC ha desarrollado (Estrategia Nacional de Inteligencia Artificial del Uruguay 2024 - 2030, 2024) siendo sus "objetivos específicos".

- Establecer un marco de gobernanza que garantice el desarrollo y uso ético, responsable y seguro de la IA
- Desarrollar las capacidades y las condiciones nacionales necesarias para fomentar y aprovechar la innovación y la aplicación de la IA.
- aprovechar la IA como motor para el crecimiento económico, el desarrollo del país, el fortalecimiento de la competitividad, la profundización del proceso de transformación digital, la mejora de la gestión y los servicios públicos, y potenciar la investigación y la innovación.

¹⁹ Orientada a la cooperación y estabilidad regional, así como la paz internacional

- Maximizar los beneficios de esta tecnología considerando impactos positivos y mitigando los posibles impactos adversos, desarrollando las capacidades para la integración de la IA.”

Y la (Estrategia Nacional de Datos 2030, 2024) teniendo por objetivos entre otros “Fomentar la disponibilidad y el uso estratégico de los datos como activo para la toma de decisiones, asegurar la adecuada protección en el uso de los datos, la mejora de la competitividad y el desarrollo de la economía basada en datos, manteniendo la soberanía digital”.

La ROU es considerada un Estado tradicionalmente neutral, con apego a las normas de la comunidad internacional y colaborante con la seguridad cooperativa mundial en el marco misiones operativas de paz de la ONU.



Figura 3. Participación histórica de la ROU en Misiones Operativas de PAZ (MOP).

Nota: Fuente Sistema Nacional de Operaciones de Paz de la ROU.

Acorde a su política de defensa nacional enfrenta amenazas híbridas: ciberataques desde actores no estatales, se identifican ingresan a través de su espacio aéreo marítimo y terrestre por parte de narcotraficantes y se detecta pesca ilegal en su Zona económica exclusiva (ZEE).

La evolución hacia entornos operativos futuros impulsados por tecnologías emergentes (EDT), según informes OEA sobre multidominio.

Uruguay, cuenta con presupuestos en defensa en el entorno del 0.8% PBI (2025).

Es menester mencionar que según el Ministerio de Defensa de Uruguay (Rendición de Cuentas, 2023) destacó el aumento en el % de la inversión (del 5 al 11%) del total del presupuesto en defensa, quedando la distribución del presupuesto: el Gasto de funcionamiento (11% aprox.), inversión (11% aprox.) y remuneraciones y retribuciones (80% aprox.) por lo que se constata aun con el incremento un desbalance.

En lo que refiere a inversión tecnológica las FFAA de la ROU enfrenta grandes brechas en lo que refiere a IA y computación cuántica.

En este sentido el Ing. Alvez W. (Comunicación personal, 2026) expresa que las nuevas tecnologías de alto impacto ofrecen un gran número de retos para la ROU, si son reguladas adecuadamente serán oportunidades de lo contrario aflorarán las amenazas, razón por la cual regularlas en un elemento clave, las tecnologías no se van a retirar llegaron para quedarse.

Análisis y discusión sobre el impacto de las EDT en los entornos operativos

Inteligencia Artificial y aprendizaje automático

El Machine Learning (ML) junto a la IA impactan directamente en la planificación estratégico operacional según (USA, 2020). Estas EDT habilitan el análisis en tiempo real de grandes volúmenes de datos²⁰; procedentes de diversos sensores y comunicaciones lo cual permite alcanzar una mejor conciencia situacional, la identificación autónoma de amenazas y en función de ello la toma de decisiones.

²⁰ A través de la Big data de sensores, imágenes satelitales, comunicaciones.

Si nos referimos a los últimos “conceptos” como las Operaciones multidominio la IA facilitara la interconexión multidominio conjunta de comando y control (JADC2)²¹, que integra el proceso de “targeting” y los sistemas autónomos en sus múltiples funciones en el entorno estratégico operacional. Ejemplo puede ser la IA generativa para simular escenarios o crear narrativas en operaciones de información²².

La IA permite elaborar narrativas para ejercer influencia en el entorno de las operaciones de información. Así mismo esto conlleva unos riesgos como los sesgos algorítmicos, la dependencia excesiva de la tecnología; teniendo como consecuencia directa lo que se podría llamar “reducción de la resiliencia humana” por lo que se hace necesario en este sentido una regulación adecuada.

Sistemas autónomos y robóticos

Los sistemas autónomos —como los drones, vehículos no tripulados²³ podrían reducir el riesgo de la mortalidad en los conflictos para los integrantes de las fuerzas armadas, aumentando así mismo la capacidad de operar en ambientes operacionales donde los sistemas Anti-acceso y Negación de Área (A2/AD) están presentes. Ejemplo de ello son los conflictos en Ucrania e Irán que han demostrado la efectividad enfrentamientos reales de alta intensidad.

En este sentido para el horizonte 2040, se visualiza que la colaboración hombre-máquina²⁴ será un estándar para el instrumento militar en condiciones operativas completas, implicando con ello contar con autonomía funcional en combate aire-aire y funciones logísticas entre otras.

Esta situación claro esta implicara que se realicen unas transformaciones en la doctrina como puntapié inicial de cualquier capacidad²⁵ doctrinarias profundas

²¹ Lo que se conoce en el mundo anglosajón como Joint All-Domain Command and Control

²² INFOOPS.

²³ Terrestres (UGV), Navales (USV) y Aéreos (UAV), incluyendo enjambres y aeronaves de combate colaborativo (CCA)

²⁴ Human-autonomy teaming

²⁵ Asociado al Marco: DOAMEPI o MIRADO -I

(Por ejemplo, pasar de fuerzas con tripuladas a fuerzas mixtas o bien predominantemente autónomas).

Computación cuántica y ciberdefensa

La computación cuántica será un desafío futuro para la ciberseguridad, esto debido a la existencia de algoritmos²⁶ que podrían inhabilitar los sistemas de cifrados.

La criptografía postcuántica es una necesidad para mitigar esta vulnerabilidad. En este mismo sentido los sensores cuánticos son oportunidades en el entorno futuro que habilitarían grandes capacidades de detección. Estas podrían ser de mucha utilidad en particular para la monitorización e identificación de navíos sumergibles o superficie.

Para la ROU y su infraestructura crítica asociada como puertos, energía, telecomunicaciones, esta situación podría llegar a materializar vulnerabilidades en el entorno cibernético, por lo que la adopción de cifrados a la altura de las nuevas circunstancias y una alineación con los estándares de gobernanza postcuántica resultan fundamentales (ejemplo los de la IEEE).

Redes de nueva generación (5G/6G), IoT militar y computación de borde

Las redes 5G/6G, el Edge Computing y el Internet de las Cosas Militar (IoMT) son tecnologías que pueden brindar conectividad de baja latencia, de alta capacidad y con buena resiliencia en entornos hostiles.

Estas tecnologías son las que sostienen la “nube de combate”, el procesamiento en el borde (edge computing) para decisiones rápidas y la distribución de sensores en el campo de batalla. Estas habilitan un análisis y procesamiento de la información próximo a donde son generados, lo que reduce la latencia y facilita decisiones en tiempo real, esto junto a la combinación de sensores dis-

²⁶ Como el de Shor

tribuidos en el entorno operativo, permite alcanzar una mejor conciencia situacional, mejora la coordinación y se obtiene una respuesta más eficiente ante las fuerzas opositoras.

En el largo plazo estas serán el sustento de la fusión de datos en tiempo real en escenarios con un alto grado de complejidad presentándose como desafío a las mismas las vulnerabilidades cibernéticas que conlleva una mayor y mejor interconexión.

Armas hipersónicas, energía dirigida y dominio espacial

Los sistemas hipersónicos tienen la capacidad de evadir los sistemas de defensa antiaérea generando una dramática reducción en los tiempos de respuesta. Así mismo las armas de energía dirigida (DEW), como láseres de alta potencia, permiten destruir drones a un bajo coste relativo.

En lo que respecta al dominio espacial, los satélites LEO (como Starlink) habilitan comunicaciones, así como también dan el soporte a la capacidad de vigilancia, si bien estas presentan vulnerabilidades a las armas antisatélite (ASAT). Esto podría materializar una oportunidad para la ROU ya podría aprovechar estas constelaciones de drones para el monitoreo de su ZEE.

Dominio cognitivo e informacional

Las operaciones de información han adquirido un papel clave en la lisa estratégica contemporánea, ya que estas están ponen foco en influir en la percepción, pudiendo afectar la legitimidad de los actores en pugna. En este sentido la IA generativa actúa como amplificador exponencial de estas capacidades, siendo un instrumento para facilitar la manipulación de las narrativas. El dominio cognitivo es actualmente un espacio de lucha en el mismo nivel de los dominios físicos, particularmente para estados democráticos requiriendo entonces una planificación y de gestión de la “infosfera”.

Impactos transversales en los entornos operativos

Optimización del ciclo OODA²⁷, dado por las capacidades de la IA y la autonomía habilitan decisiones más rápidas a las humanas particularmente si el ambiente decisional está saturado de datos, lo cual haría caer al adversario por OODA Loop.

Eliminación de la niebla del “Campo de batalla” debido al importante número de sensores interconectados en forma masiva lo que por un lado favorece la conciencia situacional y a la vez sobrecarga de información, razón por la que se hace más necesario obtener la superioridad en el dominio de la información.

Por lo anteriormente expresado el instrumento militar deben de ser capaces de sincronizar capacidades terrestres, aéreas, marítimas, espaciales, cibernéticas e informacionales ganar la batalla lo que actualmente se conoce como para Operaciones multidominio

Transformación del factor humano: el capital humano sigue siendo central, pero con mayor énfasis en la asimilación tecnológica, la colaboración hombre-máquina y el pensamiento digital. Esto plantea desafíos éticos, legales y organizacionales, particularmente en lo relativo a las reglas de empeño para sistemas autónomos.

El bajo coste de algunas EDT y el acceso a información facilitará a actores no estatales, accedan a unas capacidades que, en el pasado seria, produciéndose una “democratización del poder militar” y aumentando el fallo prospectivo por la alta imprevisibilidad.

²⁷ Observe-Orient-Decide-Act

EDT	Madurez TRL	Impacto operativo	Relevancia para Uruguay
IA ML	8	C2, targeting, INF00PS, logística autónoma	Alta: análisis inteligencia, vigilancia ZEE
Sistemas autónomos / Drones	7	Vigilancia, ataque, A2/AD, enjambres	Alta: fronteras fluviales, apoyo OMP
Computación cuántica	4	Ruptura de cifrados, sensores SIGINT navales	Media-alta: protección infraestructura crítica
5G/6G / IoMT	7	Neutralización drones, penetración defensas SAM ²⁸	Media: modernización de comunicaciones
DEW / hipersónicos	5	Comunicaciones resilientes, ISR persistente	Baja-media: vigilancia y defensa puntual
Satélites LEO	8	Comunicaciones resilientes, ISR persistente	Alta: monitoreo ZEE y operaciones ONU

Tabla 1. Tecnologías EDT seleccionadas: madurez e impacto operativo estimado (horizonte 2040)Nota: TRL = Technology Readiness Level (escala NASA 1–9). Adaptación basada en escala NASA, NATO (2026) y WEF (2026) y recopilación de consulta a expertos.

Escenarios prospectivos de operaciones futuras

Adoptando herramientas para ello 4 herramientas que apunta al 4 cardinales del diamante evidencia, experticia, interacción y creatividad; en tal sentido se utilizó las herramientas revisión literaria - Evidencia - asistida con IA, consulta a expertos -Experticia- talleres de futuros -interacción- y finalmente Wild Card como posibles escenarios no tendenciales -incluyen eventos de baja probabilidad, pero de gran impacto -Creatividad- con asistencia de IA arribándose a los siguientes escenarios.

²⁸ Misil Superficie-Aire (Surface-to-Air Missile)

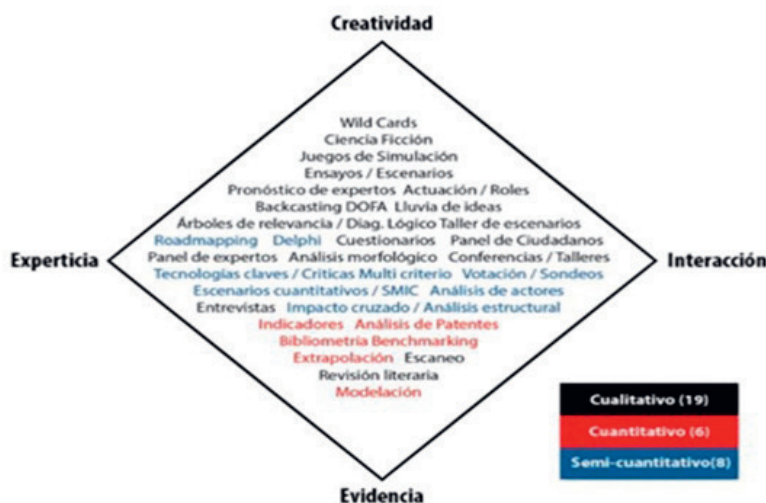


Figura 4. Diamante de Popper. Nota: Tomado de (Popper, 2011) Foresight Diamond In 21st Century Foresight.

Escenarios Futuros para el empleo del Instrumento militar 2040

- **Escenario 1: La ROU como Proveedor de Seguridad Multilateral**, este escenario se destaca por una alta cooperación internacional y protagonismo de la ROU en misiones de paz. El mismo se caracterizaría por el alineamiento con la ONU incrementando la participación en misiones de paz en diversos continentes; posicionándose como referente regional en operaciones de paz. En dicho entorno el instrumento militar de la ROU realizará Misiones complejas en ambientes urbanizados por una gran carga de actores no estatales y con la presencia de crisis humanitarias. Dichas operaciones inteligénciales combinadas se integrarán con agencias civiles y policiales lo cual requerirá una alta exigencia en interoperabilidad con fuerzas extranjeras²⁹.
- **Escenario 2: Región Fragmentada y Seguridad Regional Autónoma**, donde se destaca la presencia del debilitamiento del orden global y fortalecimien-

²⁹ Implicará que el instrumento militar se especialice, se profesionalice o bien mejore sus capacidades para participar de operaciones multinacionales (incluirá capacitación en idiomas, derechos humanos y gestión civil-militar e Incorporación de tecnologías de monitoreo y logística avanzada).

to del regional; este escenario se caracterizaría por una menor eficacia del sistema multilateral; América Latina desarrollaría mecanismos propios de seguridad y habría un Incremento de tensiones regionales (crimen organizado, migraciones, competencia por los recursos). Por lo que nos encontraríamos con un entorno operativo donde las operaciones dentro de la región estarían enfocadas en protección de fronteras, apoyo a seguridad interna, así como la presencia de Misiones de estabilización en países vecinos viéndose una significativa cooperación con fuerzas de la región. Todo ello implicaría que el Instrumento militar aumente el control territorial y fronterizo, y a la vez que se integre con fuerzas policiales y agencias estatales, debiendo desarrollar capacidades de respuesta rápida (QRF).

- **Escenario 3: Conflictos Híbridos y Dominio Tecnológico**, donde la guerra cambia hacia diferentes dominios como el ciberespacio o la “infosfera” estando presentes sistemas autónomos. Este escenario estará caracterizado por el aumento de amenazas híbridas como los ciberataques, la desinformación, el sabotaje de infraestructuras críticas identificándose Actores no estatales con significativas capacidades tecnológicas avanzadas. Este entorno operativo será testigo del campo de batalla multidominio (Tierra, ciberespacio, espacio, aéreo, marítimo, informacional) por lo que habrá un número significativo de operaciones sin contacto físico directo. Todo ello implicará para el instrumento militar la creación de unidades de ciberdefensa, el uso de inteligencia artificial para análisis y toma de decisiones y la protección de infraestructuras críticas nacionales (puertos, energía, telecomunicaciones).
- **Escenario 4: “Crisis Climática y Seguridad Humana”**, donde el cambio climático redefine el rol de las Fuerzas Armadas, este escenario se caracterizará por el Incremento de eventos extremos como, las inundaciones, sequías, crisis alimentarias, migraciones climáticas en la región, en función de ello el Instrumento Militar desarrollará Operaciones de apoyo a la población, como evacuaciones, apoyo en tareas de logística humanitaria, así como en actividades de reconstrucción, e intervención en crisis ambientales transfronterizas. En función de ello el Instrumento Militar tendrá un rol central en la gestión de emergencias y la coordinación con organismos civiles, por lo que las capacidades logísticas y de ingenieros jugarían un papel fundamental en función de los objetivos y el tipo de operaciones a desarrollar.

Síntesis de los escenarios

Todos los escenarios tienen como denominador común que:

- La ROU continuará siendo un actor internacional con una fuerte tradición institucional y participación en misiones internacionales, ajustado a las normas del derecho internacional.
- Uruguay es país con recursos limitados debiendo priorizar presupuesto de inversión en EDT particularmente para desarrollar capacidades críticas priorizando las áreas de mayor impacto como la Ciberdefensa, la Inteligencia y análisis de información, sistemas no tripulados, operaciones de información ya que las mismas serán determinantes en los entornos operativos futuros.
- Que es necesaria la formación de sus Recursos humanos, la adaptación doctrinaria y la incorporación del enfoque multidominio para de esta forma integrar capacidades cibernéticas, informacionales militares y tecnológicas.
- Se deberá realizar una adaptación presupuestal aumentando el porcentaje en inversión y dentro de la inversión en las EDT con mayor relevancia para Uruguay.
- Los hechos, tendencias, impactos y escenarios refuerzan la necesidad de adoptar enfoques estratégicos flexibles y adaptativos.

Síntesis del impacto asociados a entornos operativos futuros

En suma, las EDT transformaran los entornos operativos futuros, especialmente en los procesos de toma de decisiones, en virtud de que la velocidad de procesamiento de datos, la automatización y la superioridad informacional permiten respuestas más rápidas, reduciendo los tiempos de reacción.

En función de ello las personas asumirán roles diferentes focalizándose en la supervisión, validación y conducción estratégica de sistemas autónomos.

Esto se verá potenciado por las tecnologías de trabajo colaborativo hombre-máquina las cuales amplían las capacidades de análisis, si bien trae aso-

ciada la dependencia tecnológica, vulnerabilidades cibernéticas y fallas en la toma de decisiones automatizada

Además, de esto se suman los dilemas éticos vinculados al uso de sistemas autónomos, en el ámbito militar, donde se delegaría decisiones críticas en función de asegurar la supervivencia, todo lo cual requerirá de debate y regulaciones específicas en este sentido.

Así mismo las EDT profundizaran las asimetrías tecnológicas entre Estados y organizaciones, obligando a las instituciones a desarrollar procesos permanentes de adaptación organizacional, doctrinal y estratégica para mantener su eficacia y competitividad en los escenarios futuros.

En virtud de ello podemos decir que las EDT generan implicancias tales como:

- Reducción de los tiempos de decisión por lo que los conflictos se aceleraran
- Los entornos operativos estarán intrínsecamente interconectados por lo aumentara la complejidad de los conflictos.
- La dependencia en sistemas digitales y la necesidad desarrollar esas tecnologías sin depender de 3ero como forma de obtener independencia estratégica.
- La presencia de múltiples actores no solo estatales con acceso a capacidades de uso dual de gran impacto.

Conclusiones

Las EDTs están redefiniendo los escenarios de operaciones futuras, configurando un entorno multidominio donde la información, la velocidad en la decisión y la adaptación serán factores determinantes -si ya no los son- para el éxito. Dicha reconfiguración muestra sus primeras señales débiles en conflictos actuales, tal y como se evidenció en el análisis del presente reporte. Por lo que una comprensión oportuna de las dinámicas constituye la clave para la anticipación por parte de los actores en función de la anticipación de dicha evolución.

Entre los desafíos más relevantes a ser acometidos se destacan, los dilemas éticos vinculados a los sistemas autónomos en el marco de empleo del instru-

mento militar; particularmente a los riesgos que plantea, la autonomía funcional en el marco de la toma de decisiones en situaciones críticas sin la intervención humana³⁰ con el propósito de mejorar la eficiencia táctica. Por lo antes expresado es fundamental regular a través de marcos normativos, regulaciones que garanticen el control humano en el proceso de toma de decisiones para el empleo del instrumento militar en los entornos operativos futuros.

Alineado al marco teórico, donde la naturaleza de la guerra³¹ permanece constante a lo largo del tiempo; su carácter sí evoluciona, como consecuencia de la innovación tecnológica, la organización y el contexto histórico donde se desarrolla. Esta distinción resulta esencial para entender que la incorporación de EDTs no altera los fines del empleo de las FFAA, pero sí transforma profundamente los medios, los procesos y los dominios donde se opera.

El desarrollo de escenarios futuros no busca acertar que pasará a futuro -el fallo prospectivo es un hecho- si no orientar la acción del presente mediante el trazado de un plan estratégico, dando insumos para la vigilancia prospectiva, todo lo cual requiere observar la evolución y recalibrar los escenarios en los tiempos intermedios.

La República Oriental del Uruguay, enfrentará el desafío de adaptarse a estos entornos mediante el desarrollo de capacidades específicas asociadas a conceptos, por lo que la actualización doctrinaria y la inversión en capital humano será clave.

Asociada al punto antes mencionado la ventaja crítica en estos entornos no estará dada por la cantidad de recursos a disposición del actor considerado, sino por la capacidad de desarrollar EDTs, regularlas y explotarlas adecuadamente, manteniendo la soberanía tecnológica. En tal sentido la libertad de acción estratégica para la ROU estará en mucho correlacionada a reducir dependencias con actores externos particularmente en tecnologías con alto impacto. En este sentido y acorde al análisis realizado las oportunidades para la ROU se concentrarán en análisis de información, inteligencia, ciberdefensa, y sistemas

³⁰ Que puede incluso llegar a consecuencias de letalidad en seres humanos.

³¹ Entendida como el conjunto de elementos esenciales que le son constitutivos, como la violencia, la incertidumbre y su dimensión política.

no tripulados y operaciones de información, debido al alto grado de impacto frente a las amenazas. Para capitalizar las oportunidades mencionadas, resultaría entonces necesario una alineación progresiva con estándares internacionales y cooperación en el marco de OOI³².

Fijar y mantener estándares o lineamiento que reglamenten las tecnologías cuánticas. Estos estándares son sumamente relevantes ya que las tecnologías cuánticas impactarán directamente en:

- La criptografía y asociado a ellas las comunicaciones seguras,
- Inteligencia, procesamiento masivo de datos y toma de decisiones
- Guerra electrónica y Ciberguerra
- Navegación y posicionamiento global
- Superioridad tecnológica futura.
- Targeting

Recomendaciones

Realizar Inversiones en tecnología de uso dual, con énfasis tanto en computación cuántica como IA, explotando al máximo las capacidades institucionales de organismos como ANTEL, UTEC y AGESIC. Así mismo realizar acciones que apunten a captar financiamiento en el entorno de OOI³³. Esta articulación entre capacidades nacionales y cooperación internacional permitiría reducir la brecha tecnológica y al mismo tiempo no perder independencia estratégica.

Fortalecer y ampliar los espacios de intercambio y o cooperación con OOI y actores regionales³⁴ en el marco de mecanismos de cooperación hemisférica como la OEA, los cuales podrían brindar espacios de intercambio de experiencias o bien realizar ejercicios conjunto-combinados en materia de: ciberdefensa, drones e interoperabilidad multidominio, entre otras. Estos espacios serian

³² Por ejemplo, OEA

³³ Ejemplo la OEA.

³⁴ Como por ejemplo Brasil y Argentina.

una oportunidad para elevar el nivel de preparación de la Fuerzas Armadas (FFAA), reducir brechas de capacidades, sin generar dependencia estratégica.

Actualizar la Política Militar de Defensa, en particular el concepto de empleo estratégico de las FFAA, con el fin de lograr alineamiento estratégico entre la doctrina y los avances tecnológicos identificados, particularmente buscando garantizar la coherencia entre los conceptos operativos adoptados y las capacidades efectivamente disponibles / proyectadas y estas con la evolución de las EDTs.

Implementar en el ámbito del Sistema de Enseñanza Militar, programas de formación de nivel estratégico militar, orientados al análisis de las EDT para la defensa, abordando las bases conceptuales fundamentales de las tecnologías prioritarias³⁵ y sus implicancias estratégicas, éticas y doctrinarias para el empleo de las FFAA. El propósito sería generar la capacidad en el Cuerpo de Oficiales para analizar y asesorar acerca de la integración tecnológica, en los procesos de toma de decisiones al más alto nivel.

Potenciar la formación de oficiales en el exterior, particularmente en desarrollo de conceptos operativos, planeamiento por capacidades y procesos de transformación tecnológica en el ámbito de la defensa. En función de ellos, capitalizar estos conocimientos para fortalecer las capacidades de Planeamiento de Nivel Estratégico Militar. Esta inversión en recursos humanos está en línea con lo señalado anteriormente³⁶ a que la ventaja crítica en los entornos operativos futuros no dependerá de la cantidad de recursos, sino de la capacidad de comprender e integrar las EDTs en forma oportuna.

Se recomienda enmarcar la gestión tecnológica del Instrumento militar en base a estándares internacionales como por ejemplo, los que establece IEEE (2026) para la gobernanza en tecnologías cuánticas que comprenden entre otras, la Seguridad de Redes Post-Cuántica³⁷ (P1943), la Ciberseguridad Cuán-

35 Como, por ejemplo: La inteligencia artificial, los sistemas autónomos, la computación cuántica y la ciberdefensa.

36 En las conclusiones.

37 Estándar IEEE P1943™: Define una versión optimizada postcuántica de los protocolos de seguridad de red.

tica³⁸ (P1947), la Computación Híbrida Cuántica-Clásica³⁹ (P3185), la Computación Cuántica y la Eficiencia Energética de Simulación⁴⁰(P3329) y la terminología específica de las tecnologías cuánticas⁴¹(P 7130). Adoptar estos estándares para las tecnologías cuánticas permitirá una adecuada gobernanza tecnológica, mejorando la interoperabilidad con actores cooperantes y socios estratégicos, todo lo cual fortalecerá la ciberseguridad postcuántica, (incluyendo las comunicaciones cuánticas y la criptografía postcuántica) de esta manera se aseguraría un desarrollo responsable de las EDTs. Este punto cobra particular relevancia para la ROU, debido a la necesidad de proteger su infraestructura crítica⁴², esto en función de que durante el análisis fue una de las vulnerabilidades identificadas.

Desarrollar “Gap análisis” con el propósito de identificar la brecha entre las capacidades tecnológicas actuales del instrumento militar y las capacidades requeridas para actuar eficazmente en los entornos operativos futuros -horizonte 2040- y en función de los resultados desarrollar un plan que permita alcanzar las capacidades tecnológicas de mayor impacto para la ROU- ciberdefensa, inteligencia, sistemas no tripulados y operaciones de información- contemplando fases e hitos, los cuales permitan evaluar, revisar y recalibrar. El mismo, debería contener vasos comunicantes con el ciclo de planeamiento de la defensa y ser coherente con los presupuestos que se vayan sucediendo.

Incrementar la inversión en EDTs con prioridad en la formación y desarrollo de capacidades ciberdefensa cognitiva⁴³ y C4ISR -mando, control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento- de uso dual, para generar las condiciones necesarias que permitir aprovechar las capacidades tecnológicas existentes en la ROU. Este proceso deberá ser complementado con el

³⁸ Estándar IEEE P1947™: Describe un Marco de Ciberseguridad Cuántica.

³⁹ Estándar IEEE P3185™: Define la arquitectura de hardware y software de entornos híbridos de computación cuántica-clásica.

⁴⁰ Norma IEEE P3329™: Define una eficiencia energética universal para la computación cuántica y la simulación.

⁴¹ Norma IEEE P7130™ Esta norma aborda la terminología específica de las tecnologías cuánticas y establece definiciones necesarias para facilitar la claridad de comprensión y facilitar la compatibilidad e interoperabilidad.

⁴² Puerto, energía y telecomunicaciones.

⁴³ Apuntando a aumentar la resiliencia informacional considerando el riesgo de la desinformación a gran escala.

delineado y desarrollo de alianzas público-privadas a través de organismos (como ANTEL y la UTEC) y stakeholders del sistema Ciencia - Tecnología e Innovación. En este sentido el desarrollo de tecnologías postcuánticas deberá ser un eje fundamental de inversión dado el impacto multiplicador que genera sobre la inteligencia la ciberseguridad y las comunicaciones a futuro.

Bibliografía

- Agencia de gobierno electrónico y sociedad de la información del conocimiento. (2024). *Estrategia Nacional de Inteligencia Artificial del Uruguay 2024 - 2030*. Montevideo: AGESIC.
- AGESIC. (2024). *Estrategia Nacional de Datos 2030*. Montevideo: AGESIC. Obtenido de <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-datos-del-uruguay-2030/estrategia-nacional-datos-0>
- Alvez, W. (22 de Mayo de 2026). Comunicación personal. Montevideo.
- Australian Strategy Policy Institute. (2023). *ASPI's Critical Technology Tracker*. Canberra: ASPI.
- Clausewitz, C. V. (1832). *De la guerra*. Buenos Aires: Librodot.
- Freedman, L. (2013). *Strategy: A history*. Oxford: Oxford University Press.
- Gray, C. (2010). *The strategy bridge: Theory for practice*. Oxford: Oxford University Press.
- IEEE.org. (20 de Mayo de 2026). *IEEE Standards & Projects for Quantum Technologies*. Obtenido de IEEE: <https://standards.ieee.org/ieee/1947/11583/>
- Instituto Internacional de Derecho Humanitario de Ginebra. (2025). *Un campo de batalla cambiante*. Obtenido de <https://blogs.icrc.org/law-and-policy/es/2025/06/03/un-campo-de-batalla-cambiante-tecnologia-tacticas-y-limites-cada-vez-mas-difusos-en-el-ambito-de-la-guerra/>
- Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla*. London: Oxford University Press.
- Ministerio de Defensa Nacional - Uruguay. (13 de Julio de 2023). *Rendición de Cuentas*. Obtenido de Ministerio de Defensa Nacional: <https://www.gub.uy/ministerio-defensa-nacional/comunicacion/noticias/ministro-garcia-resalto-duplicacion-inversiones-defensa-jerarquizacion>

- NATO. (2022). *Strategic Concept*. Madrid: NATO. Obtenido de <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>
- NATO. (20 de Mayo de 2026). *NATO - Emerging and Disruptive Technologies*. Obtenido de Emerging and disruptive technologies: <https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies>
- Popper, R. (2011). *Foresight Diamond In 21st Century Foresight*. Manchester: University of Manchester.
- Rahman, E. M. (3 de Septiembre de 2024). *ISACA.org*. Obtenido de Emerging Technology: Key Challenges and Opportunities: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-17/emerging-technology-key-challenges-and-opportunities>
- Real Instituto Elcano. (2019). *Desarrollos tecnológicos militares frente a nuevos conceptos operativos*. Madrid: RIE. Obtenido de <https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari86-2019-desarrollos-tecnologicos-militares-frente-nuevos-conceptos-operativos.pdf>
- Soto, M. (2023). *Nuevas tecnologías en el contexto global de seguridad: la oportunidad frente al desafío*. Madrid: IEEEES.
- Taleb, N. N. (2007). *The Black Swan*. New York: Random House.
- (2024). *Tecnologías de alto impacto para la defensa en el entorno operativo 2035*. Madrid: Ministerio de Defensa. Obtenido de https://emad.defensa.gob.es/Galerias/CCDC/files/tecnologias_de_alto_impacto.pdf
- Toffler, A. (1979). *La Tercera Ola*. (A. Martín, Trad.) Nueva York: Bantam Books.
- UK. (2018). *Global Strategic Trends* (6ta ed.). London: Ministry of Defence UK. Obtenido de https://assets.publishing.service.gov.uk/media/66f6d04cc71e42688b65ee14/GST_the_future_starts_today_ARCHIVE.pdf
- Uruguay. (2020). *Política de Defensa Nacional Decreto 371/20*. Montevideo.: CODE-NA.
- USA. (2020). *Future Operational Environment:Forging the Future in an Uncertain World 2035-2050*. Washington, D.C.: U.S. Army Futures Command.
- World Economic Forum. (2026). *Global Risks Report* . Geneva: WEF.

